SIEMENS

HiPath AP 1140

H.323 Terminal

Operation and
Administration Manual
Version 3.0

HiPath

Copyright © Siemens AG, 1999-2001

All rights reserved.

HiPath is a trademark of Siemens Aktiengesellschaft.
All other brand and product names may be trademarks of their respective holders.

Siemens AG provides this documentation without any warranty of any kind, either implied or expressed, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose.

Contents

Introduction v

Before you Begin v
Acronyms vi

Getting Started 1

Overview 1
Features 2
Panels 4
Interpreting the HiPath AP 1140 LEDs 6

Installation 9

Hardware and Software Requirements 9
Choosing a Suitable Location 9
Setting up the HiPath AP 1140 for the First Time 10
Installing the HiPath AP 1140 Hardware 15

Basic Configuration 17

Web Interface 17
Integrating the HiPath AP 1140 into the Communication Environment 23
Configuring IP Addresses 27
Changing the Password/User Name 29

Registering to a Gatekeeper 33

Setting up Gatekeeper Information 33
Gatekeeper Registration Logic 35

Ports Configuration 45

Configuring Incoming and Outgoing Calls Parameters 45

Miscellaneous Configuration 55

Quality of Service Settings 55
Geographical Specific Configuration 62
SNTP Settings 66
Viewing Hardware Information 67
System Failure Bypass Activation Section 68
Advanced Debugging 69

How to Use the HiPath AP 1140 73
HiPath AP 1140 Call Processes 73
Using Dialing Rules 77
Dialing Rules Examples 80

Software Upgrade 83
Setting up Software Download 83
Emergency Software Download Configuration Section 85

Maintenance 89
Warning 89
Caution Regarding Handling 89
Troubleshooting 90

Appendix A – DHCP Server Vendor Specific Information 95
Configuring the DHCP Server 95

Appendix B – Country Specific Parameters 101
Austria 101
France 101
Germany 102
Great Britain 103
Italy 103
North America 104
Spain 105
Switzerland 105
Europe 106

Appendix C – Safety & EMI Certifications 107
Safety & EMI Certifications Supported 107
Disclaimers 107

Appendix D – Glossary 111

Introduction

The HiPath AP 1140 provides multiplexed IP connectivity for up to four analog telephones or fax machines to a Local Area Network with access to an Intranet or the Internet to permit high-quality, full duplex, audio/fax communications over IP Packet Networks.

Before you Begin

This manual provides all the information needed to install and manage the HiPath AP 1140 with the configuration web pages. It is intended to be used by network administrators who install and set up network equipment; consequently, it assumes a basic working knowledge of LANs (Local Area Networks).

From the perspective of the LAN administrator, a HiPath AP 1140 presents itself just like another PC that is to be added to the LAN. It requires the same kind of TCP/IP addressing that is required by a PC. The HiPath AP 1140 can also use a DHCP server on the LAN to automatically receive its IP configuration assignment.

What’s New in this Version

- The web server port is now 8085. See “Setting up the HiPath AP 1140 for the First Time” on page 10 and “Accessing the Web Interface” on page 17 for more details.
- Speed dialing allows to dial an IP address & IP Address + E.164 alias. See “Accept Phone/Fax to IP Network Call Settings” on page 49 for more details.
- Explanations on the Advaced debug page. See “Advanced Debugging” on page 69 for more details.
- Lightweight registration in the Gatekeeper registration process. See “Setting up Gatekeeper Information” on page 33 for more details.
- “Telephony Settings” on page 51“Telephony Settings” on page 46 for more details.
- The Data stream transmission priority queuing media for the Differentiated Service Configuration filter has been refined in Voice stream and Fax/Modem stream transmission settings. See “Differentiated Services (DiffServ) Section” on page 56 for more details.
- The Data stream transmission priority queuing for the 802.1q configuration has been refined in Voice stream and Fax/Modem stream transmission settings. See “802.1q Section” on page 58 for more details.
- Call Forward Settings. See “Call Forward Settings” on page 53 for more details.
- H.450.2 Call Transfer (passive). The HiPath AP 1140 can act as the transferred and the transferred to entity. The HiPath AP 1140 cannot initiate a call transfer (transferring entity).
- You can select pre-defined time zones or create your own custom time zone. See “Geographical Specific Configuration” on page 62 for more details.
- You can connect to a SNTP server to receive SNTP information. See “SNTP Settings” on page 66 for more details.
- The HiPath AP 1140 can transmit Caller ID information.
- Out of band DTMF. See “Features” on page 2 for more details.
- Progress Message. See “Features” on page 2 for more details.

Acronyms

DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
FXS	Foreign Exchange Service
IP	Internet Protocol
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Media Access Control
Mb/s	Megabits per Second
PBX	Private Branch Exchange
PCM	Pulse Code Modulation
PROM	Programmable Read-Only Memory
PSTN	Public-Switched Telephone Network
SCN	Switched Circuit Network
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
VoIP	Voice Over Internet Protocol
WAN	Wide Area Network

Getting Started

This chapter introduces the HiPath AP 1140. It describes its features and illustrates its front panel indicators and back panel connectors.

Overview

The HiPath AP 1140 is an IP telephony adaptor that connects up to four (4) analog terminals to a LAN with access to an IP Network, allowing high-quality, full duplex, audio/fax communication.

Why use the HiPath AP 1140?

There are many reasons to use the HiPath AP 1140:

- Merges voice and data traffic onto a single unified network.

  Carrying telephone traffic over data networks uses less bandwidth (as compared to telephone trunks), resulting in a more cost-effective network solution.
- Easily integrates with existing telephone equipment.

  Overhead is minimal, because the HiPath AP 1140 fully utilizes your existing telecommunications equipment and computer networks.
- Bypasses long-distance toll charges for realized savings.
- Supports 10 Mb/s and 100 Mb/s Ethernet networks.
- Upgrades software easily for future enhancements.
- Uses the latest standards in Internet Telephony.
- Supports the following Codecs:
  - G.711 (µ-law, A-law)
  - G.723.1 (5.3 kbps and 6.4 kbps)
  - T.38 (fax)
- Supports Quality of Service technologies.
  - Differentiated Services (DS) Field
  - IEEE 802.1q user priority tagging

How does it Work?

When an Internet telephony call is placed from one location to another, the voice signals pass through the HiPath AP 1140 connected to the handset in the caller’s area. They are compressed into data packets, which are then diverted by the HiPath AP 1140 onto an IP/data network such as the Internet, or another type of data network. Upon reaching its destination, the voice data is converted back into voice signals, then fed into the corresponding telephone or fax machine.

The HiPath AP 1140 system utilizes technology that optimizes available bandwidth, so users do not hear echoes, stops and starts, or annoying clicks and pops. When traffic congestion is properly managed, HiPath AP 1140 customers cannot tell that their conversation is being carried over a packet network rather than the traditional SCN.

See “HiPath AP 1140 Call Processes” on page 73 for more details.

Features

The following table lists some of the features the HiPath AP 1140 offers.

Feature	Description
4 FXS Ports	Four central office quality subscriber’s line interface circuits (SLICs) supporting all the BORSCHT (**B**attery feed, **O**ver-voltage protection, **R**inging, **S**ignaling, **C**oding, **H**ybrid, and **T**esting) functions and thus meet most world wide telephony standards.
Fax Interface	Handles G3 and Super G3 fax transmissions at speeds up to 33.6 kbps. Automatic fax mode detection is standard. Real-Time Fax over TCP in clear channel with the T.38 protocol stack is also available (Non-Standard capabilities).
Analog Modem	Supports 9.6 kbps to 33.6 kbps analog modems (V.34 support over clear channel). Modems with higher rate capabilities (e.g.: V.90) will automatically fall back, if configured adequatly, in the transmission range supported, usually near 33.6 kbps.
Compliant with H.323 FastConnect	The H.323 FastConnect procedure is an enhancement feature introduced in the H.323v2 protocol to reduce the initialisation latency when initiating a call. To operate in FastConnect mode, all H.323 elements (calling party, caller party, gatekeeper) involved in the call setup activity must comply to the FastConnect procedure. Otherwise, the normal initialisation procedure takes place.
Supports the PhoneMail System	You can connect the HiPath AP 1140 to Siemens AG PhoneMail system. OSCAR non-standard capability is supported.

Feature	Description
Supports H.450.2 Call Transfer (passive)	The HiPath AP 1140 can act as the transferred and the transferred to entity. It cannot initiate a call transfer (transferring entity).
Compliant with the AutoDiscovery feature	The HiPath AP 1140 is compliant with the HiPath Gatekeeper's AutoDiscovery feature. Hipath Gatekeepers will thus be able to discover HiPath AP 1140 units on the network. This allows to build a "Network map" of all the units that support the "Autodiscovery". The "Network Map" is a menu in the gatekeeper. In a second phase, when a unit has answered the first autodiscovery message, the "Autodiscovery" feature sends a second message which is the configuration that this unit must use. Note that this works only for the QoS parameters.
Out of band DTMF	The HiPath AP 1140 can receive and send out of band DTMFs using the H.245 UserInputIndication message. The HiPath AP 1140 includes the following features in its capability set: – Receive and transmit DTMF capability – Receive and transmit capability – Transmit iA5String capability Note that out of band using RTP is not supported.
Progress message	The HiPath AP 1140 supports Progress messages, which may be sent by an endpoint or Gatekeeper to indicate the progress of a call in the event of interworking with the SCN.
RTCP	The HiPath AP 1140 supports the Real Time Control Protocol, which is used to send packets to convey feedback on quality of data delivery.
Caller ID	The HiPath AP 1140 can transmit Caller ID information.
System Failure Bypass	In the event of a commercial power failure or network failure, the bypass feature permits users to make and receive calls even when the HiPath AP 1140 is not operating. See "System Failure Bypass Activation Section" on page 68 for more details.
Fully Configurable "SCN-Like" Experience	Provides all the usual tones normally heard on the standard telephone network. It also provides country-specific tones and ringer types. For example, a dial tone will be heard as soon as the handset is lifted. Call progress tones such as ringback and busy are also provided.

Feature	Description
Remote Site Configuration/ Management	The HiPath AP 1140 is integrated seamlessly into your existing administration environment. Implementation of a HTTP server allows device-related adjustment parameters to be modified and polled remotely. The software upgrade is downloaded via a TFTP server.

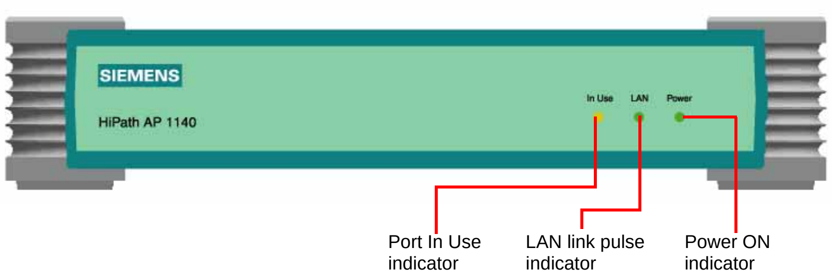
Panels

This section provides an overview of the HiPath AP 1140’s front and rear panels.

Front Indicators

Figure 1 shows the three (3) visual indicators located on the front of the HiPath AP 1140.

Figure 1: HiPath AP 1140 Front Panel Indicators



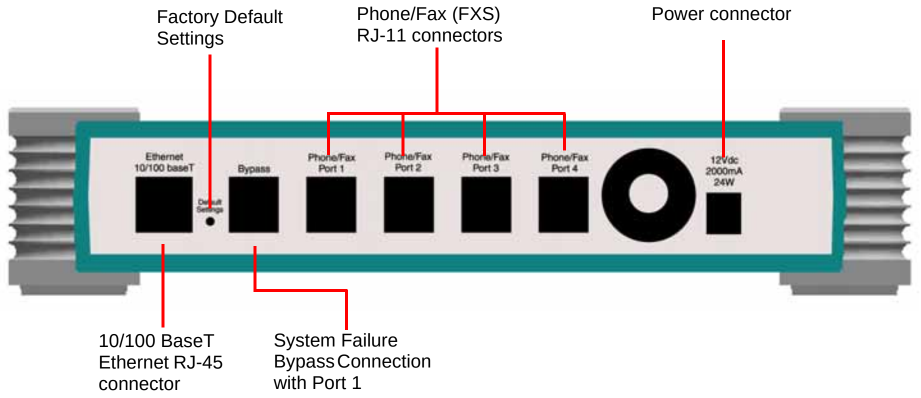
The following message describes the LEDs on the front panel of the HiPath AP 1140.

Indicator	Description
– **In Use** – Port In Use indicator	When lit, at least one of the FXS ports is in use.
– **LAN** – LAN link pulse indicator	Provides the state of the network connected to the *Ethernet* port.
– **Power** – Power ON indicator	When lit, power is applied to the HiPath AP 1140.

Rear Connections

Figure 2 shows the back panel connectors of the HiPath AP 1140.

Figure 2: HiPath AP 1140 Back Panel Connectors



The following message describes the back panel connections.

Connection	Description
Ethernet	A 10/100 BaseT Ethernet RJ-45 connector for access to a LAN.
System Failure Bypass	In the event of a commercial power failure or network failure, the bypass feature permits users to make and receive calls even when the HiPath AP 1140 is not operating. See "System Failure Bypass Activation Section" on page 68 for more details.
Phone/Fax Port 1 Phone/Fax Port 2 Phone/Fax Port 3 Phone/Fax Port 4	Four (4) RJ-11 connectors to attach a conventional telephone or G3/Super G3 fax machine.
Power connector	A power connector for the power supply of the HiPath AP 1140.
Default Settings	The *Default Settings* switch resets configuration parameters of the HiPath AP 1140 to factory default (known) values. It can be used to reconfigure the unit. See "Setting up the HiPath AP 1140 for the First Time" on page 10 for more information.

Interpreting the HiPath AP 1140 LEDs

The HiPath AP 1140 has three (3) LED indicators located on the front panel, which are identified as *In Use*, *LAN*, and *Power*. A LED can have three states: On, Off and Blinking.

In Use LED

The *In Use* LED provides status on the FXS port use.

LED Status	Description
Steady OFF	No ports are in use.
Steady ON	At least one port is in use.

LAN LED

The *LAN* LED provides the status of the network connected to the *Ethernet* port. Normal operation is variable On-Off blinking.

LED Status	Description
Steady OFF	*Ethernet* port does not sense the carrier signal.
Steady ON	*Ethernet* port does sense the carrier signal.

Power LED

The *Power* LED is used to indicate whether the HiPath AP 1140 is operational at its most basic level. It does not imply that the unit can be used, only that it is capable of being used. Normal operation is steady On.

LED Status	Description
Steady ON	Power is on and the unit does not have any major failure
3 Hz Blinking at 50% on duty cycle	Failure of power-up diagnostics such that the unit is unable to operate.
1 Hz Winking at 75% on duty cycle	Failure of DHCP – no acceptable offer received from DHCP.
Steady OFF	The unit has no power supply input.

LED Behavior in Download Mode

When the HiPath AP 1140 initiates a software download, the three LEDs located on the front panel are used to report the status of the process.

Event	LED State
Image downloading	Each LED blinks alternately at 1 Hz with 1/3 ON duty cycle.
Image writing (writing to EEPROM phase)	*LAN* LED ON, *Power* LED OFF. **Warning**: Do not turn the HiPath AP 1140 off while in this state.
Image download failed	All LEDs blink at the same time at 2 Hz with 50% ON duty cycle for 4 seconds.
Image download completed successfully	All LEDs ON.

Installation

This chapter lists the hardware and software requirements of the HiPath AP 1140. It also describes how to install the HiPath AP 1140 hardware.

Hardware and Software Requirements

The HiPath AP 1140 requires the following items:

Item	Description
Phone/Fax	A standard telephone or fax attached to a FXS port of the HiPath AP 1140. One (1) to four (4) phones or faxes can be attached to the HiPath AP 1140.
Remote Party	Endpoints where the HiPath AP 1140 terminates a call. For example, it could be: – a standard telephone/fax attached to a terminal such as a HiPath AP 1100, another HiPath AP 1140, etc. – a PC Client such as the HiPath ComDesk – an IP phone directly connected to the IP network – etc.
DHCP Server	This server supplies all network parameters to the HiPath AP 1140 such as the IP address and subnet mask.
TFTP Server	Necessary for software updates.
Syslog Daemon (optional)	The Syslog daemon receives all status messages coming from the HiPath AP 1140.

Choosing a Suitable Location

The HiPath AP 1140 is suited for use in an office environment where it can be free standing on its rubber feet.

When deciding where to position the HiPath AP 1140, ensure that:

- The HiPath AP 1140 is accessible and cables can be connected easily.
- The cabling is away from the following:
  - Sources of electrical noise such as radios, transmitters, and broadband amplifiers.

  - Power lines and fluorescent lighting fixtures.
  - Water or moisture that could enter the casing of the HiPath AP 1140.
- The airflow is not restricted around the HiPath AP 1140 or through the vents in the side of the unit. It is necessary to have a minimum of 25 mm (1 in.) clearance.
- The fan on the HiPath AP 1140 is not blocked or the back of the unit is not too close to the wall.

Setting up the HiPath AP 1140 for the First Time

Upon delivery, the HiPath AP 1140's default network parameters are not properly set to be used right away on your network. When setting up the HiPath AP 1140 for the first time, you must change these settings so that it can access your network.

During the first installation of the HiPath AP 1140, the straightforward way to access the configuration web pages is to connect a PC and the unit to the same hub (without connecting the hub to a network). The configuration web pages can thus be directly accessed with an Internet browser running on the PC.

You can also connect the HiPath AP 1140 directly to the network card of a PC with an Ethernet 10/100 BaseT crossover cable.

Using the Default Settings Switch

You should use the Default Settings switch in the following cases:

- When setting up the HiPath AP 1140 for the first time.
- In case of emergencies, i.e. when the HiPath AP 1140 refuses to work properly for any reason or the connection to the network is lost.

Using the Default Settings switch when booting the HiPath AP 1140 will assign static default IP addresses. The configuration web pages can thus be directly accessed with an Internet browser running on the PC.

▶ **To use the Default Settings switch:**

1. With a 10/100 Hub and two (2) 10/100 BaseT Ethernet RJ-45 straight cables, connect both cables to the Hub; one of them is connected into the *Ethernet* connector of the HiPath AP 1140 and the other links the computer to the Hub.

   Alternatively, you can connect a Ethernet 10/100 BaseT crossover cable into the *Ethernet* connector of the HiPath AP 1140 and connect the other end to your computer.

2. Reconfigure the IP address of your computer to *192.168.0.10* and enter the Subnet Mask of *255.255.255.0*. Reboot your computer.

   Configuring the IP address of your computer to 192.168.0.10 allows you to readily receive Syslog daemon messages and download a software version, because the default IP address for Syslog daemon and software server is 192.168.0.10.

3. Insert a small paper clip into the Default Settings switch hole of the HiPath AP 1140.

   When the HiPath AP 1140’s configuration is unknown, the Default Settings switch must be depressed for about 5 seconds while the HiPath AP 1140 reboots so it reverts back to a known configuration. The Default Settings switch is located at the back of the HiPath AP 1140.

4. While depressing the Default Settings switch, power the HiPath AP 1140 on by connecting the power cable to an electrical outlet and then plugging the power connector to the HiPath AP 1140.If you are using the LAN-powered option, connect the 10/100 BaseT Ethernet RJ-45 cable into the *Ethernet* connector of the HiPath AP 1140 and connect the other end to the network

> ! The electrical outlet shall be installed near the HiPath AP 1140 so that it is easily accessible.

   The Factory Default Settings must be performed when powering the HiPath AP 1140 on for the very first time, even if the HiPath AP 1140 is connected to a LAN with a DHCP server. Otherwise, the HiPath AP 1140 falls into an error state. When the HiPath AP 1140 is in an error state, the In Use indicator flashes.

   During the Factory Default Settings, the following default parameters are assigned to the HiPath AP 1140:

   - **Default local IP address**: 192.168.0.1
   - **Default subnet mask**: 255.255.255.0
   - **Syslog daemon**: 192.168.0.10
   - **Software server**: 192.168.0.10

   The default local IP address allows you to access the configuration web pages of the HiPath AP 1140 to set its different IP and hardware parameters. The following chapters explain how to use these configuration web pages.

5. If you are setting up your device for the first time, see “Setting up the HiPath AP 1140 for the first time:” on page 12.

6. When the HiPath AP 1140 has finished rebooting, turn it off, plug it on the network, and turn it on again.

> When rebooting in normal mode of operation after the factory default settings mode, the local IP address and subnet mask revert to their original value or what the DHCP sends if you are using a DHCP.

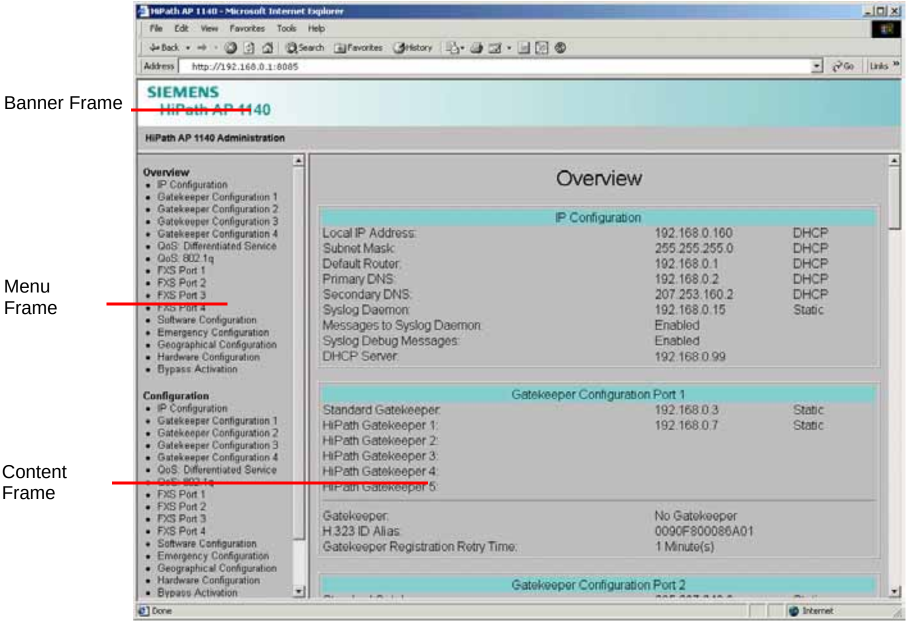
▶ **Setting up the HiPath AP 1140 for the first time:**

1. Once the HiPath AP 1140 is started, enter the IP address *192.168.0.1:8085* in the web browser of the computer connected to it.

> The web server port is 8085. When entering an IP address to reach a HiPath AP 1140, you must always put ":8085" after the IP address.

You should now see the *Overview* web page.

Figure 3: Configuration Web Pages


Banner Frame
Menu Frame
Content Frame
HiPath AP 1140 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.0.1:8085
Go Links
SIEMENS
HiPath AP 1140
HiPath AP 1140 Administration
Overview
IP Configuration
Gatekeeper Configuration 1
Gatekeeper Configuration 2
Gatekeeper Configuration 3
Gatekeeper Configuration 4
QoS: Differentiated Service
QoS: 802.1q
FXS Port 1
FXS Port 2
FXS Port 3
FXS Port 4
Software Configuration
Emergency Configuration
Geographical Configuration
Hardware Configuration
Bypass Activation
Configuration
IP Configuration
Gatekeeper Configuration 1
Gatekeeper Configuration 2
Gatekeeper Configuration 3
Gatekeeper Configuration 4
QoS: Differentiated Service
QoS: 802.1q
FXS Port 1
FXS Port 2
FXS Port 3
FXS Port 4
Software Configuration
Emergency Configuration
Geographical Configuration
Hardware Configuration
Bypass Activation
Done
Internet

Overview

IP Configuration		
Local IP Address:	192.168.0.160	DHCP
Subnet Mask:	255.255.255.0	DHCP
Default Router:	192.168.0.1	DHCP
Primary DNS:	192.168.0.2	DHCP
Secondary DNS:	207.253.160.2	DHCP
Syslog Daemon:	192.168.0.15	Static
Messages to Syslog Daemon:	Enabled	
Syslog Debug Messages:	Enabled	
DHCP Server:	192.168.0.99	

Gatekeeper Configuration Port 1		
Standard Gatekeeper:	192.168.0.3	Static
HiPath Gatekeeper 1:	192.168.0.7	Static
HiPath Gatekeeper 2:		
HiPath Gatekeeper 3:		
HiPath Gatekeeper 4:		
HiPath Gatekeeper 5:		
Gatekeeper:	No Gatekeeper	
H.323 ID Alias:	0090F800086A01	
Gatekeeper Registration Retry Time:	1 Minute(s)	

Gatekeeper Configuration Port 2

2. Click the *IP Configuration* link of the *Configuration* web page in the left frame.

You will be asked a user name and password. Type **HiPathAdm** as user name and **8749Trix** as password. The User Name and Password are case sensitive hence they must be entered as shown above. See "Accessing the Configuration Web Page" on page 19 for more details.

You will gain access to the *Configuration* web page. Various choices are available for the IP address parameters of the HiPath AP 1140:

- You can decide to use only the IP addresses provided by a DHCP server.
- You can decide to use only static IP addresses that you specify.
- You can decide to use a mix of static IP addresses that you specify and IP addresses provided by a DHCP server.

3. If you do not have a DHCP server, make sure that you enter the following parameters:

   - Local IP address assigned to this HiPath AP 1140. This IP address must be *192.168.0.1*
   - Subnet mask IP address, which should be *255.255.255.0*

   Make sure that these fields are set as *Static* (the *Static* check box must be checked).

   Siemens AG recommends to print out a copy of the *Configuration* web page.

4. Click *Update* to apply the changes.

   The HiPath AP 1140 will reboot with the new information that was just entered (this will take about 10-20 seconds).

5. When the HiPath AP 1140 has finished rebooting, turn it off, plug it on the network, and turn it on again.

> When rebooting in normal mode of operation after the factory default settings mode, the local IP address and subnet mask revert to their original value or what the DHCP sends if you are using a DHCP.

▶ **To exit an error state:**

1. Power off the HiPath AP 1140 by unplugging the power connector.
2. Insert a small paper clip into the Default Settings switch hole.

3. While depressing the Default Settings switch, power the HiPath AP 1140 back on by plugging the power connector.

> ℹ The Default Settings switch can always be used to configure or reconfigure the HiPath AP 1140.

Finding the IP Address Assigned to an HiPath AP 1140

You do not know the IP address assigned by the DHCP server to the HiPath AP 1140 if:

- You have not previously reserved an IP address in the DHCP server for a specific MAC address
- You have chosen not to use static IP addresses.

Once the HiPath AP 1140 is connected to a compatible Ethernet interface that supplies TCP/IP network access (e.g. router, switch, hub or computer), you must find its IP address to access its configuration web pages. You will need the MAC address of the specific HiPath AP 1140 for which you want to know the assigned IP address. The MAC address is printed on the label located on the bottom side of the HiPath AP 1140.

There are two ways to find an IP address:

- by using the Syslog daemon

  This must be done after reverting to factory default settings. Otherwise you will not be able to access the web pages to specify an IP address for the Syslog daemon.

- by looking into the DHCP server of your network

  Siemens AG recommends to reserve an IP address in the DHCP Server **before** installing the HiPath AP 1140 on the network. You will need the HiPath AP 1140's MAC address as unique identifier.

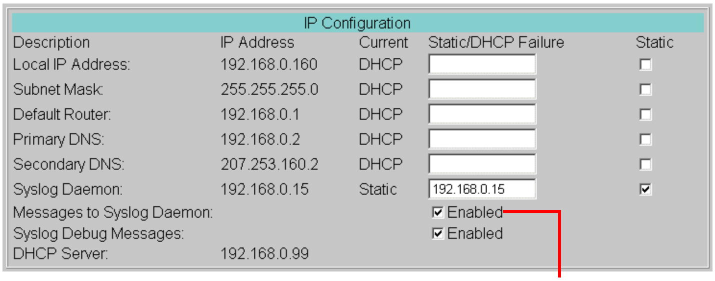
▶ **To find the IP address with the Syslog daemon:**

1. In the *Configuration* page, go to the *IP Configuration* section and enter the IP address of the server running the Syslog daemon. Make sure that you check the *Static* option on the right.

   See “Configuring IP Addresses” on page 27 for more information on the Syslog daemon.

2. Enable *Messages to Syslog Daemon*.

Figure 4: Syslog Daemon



IP Configuration				
Description	IP Address	Current	Static/DHCP Failure	Static
Local IP Address:	192.168.0.160	DHCP		☐
Subnet Mask:	255.255.255.0	DHCP		☐
Default Router:	192.168.0.1	DHCP		☐
Primary DNS:	192.168.0.2	DHCP		☐
Secondary DNS:	207.253.160.2	DHCP		☐
Syslog Daemon:	192.168.0.15	Static	192.168.0.15	☑
Messages to Syslog Daemon:			☑ Enabled	
Syslog Debug Messages:			☑ Enabled	
DHCP Server:	192.168.0.99			

Click here to enable messages to the Syslog daemon

3. Click *Update* to apply the changes.
4. Once the HiPath AP 1140 has restarted (this could take 10 to 20 seconds), turn it off, connect it to your network and turn it on again.
5. With the Syslog opened, watch the HiPath AP 1140 restart. Messages are sent to the Syslog daemon and their source is displayed. This IP address is the one assigned to the HiPath AP 1140.

This procedure will only work for one HiPath AP 1140 at a time. If you are booting several HiPath AP 1140 or similar units (RG 2100 or AP 1100), you will have no way to tell which IP address belongs to which HiPath AP 1140.

▶ **To find the IP address with the DHCP Server of your network:**

1. Open the DHCP Server you are using.
2. Browse through the list of IP addresses and find the one associated to the MAC address of the HiPath AP 1140.

   Browsing through the list of IP addresses can take some time.

Installing the HiPath AP 1140 Hardware

The HiPath AP 1140 telephone line interface has been designed to interface with a conventional analog phone. Connections to certain PBX / Key systems supply a higher line voltage that could damage the HiPath AP 1140.

Do not connect the HiPath AP 1140 directly to Analog Telephone Systems.

▶ **To install the HiPath AP 1140 hardware:**

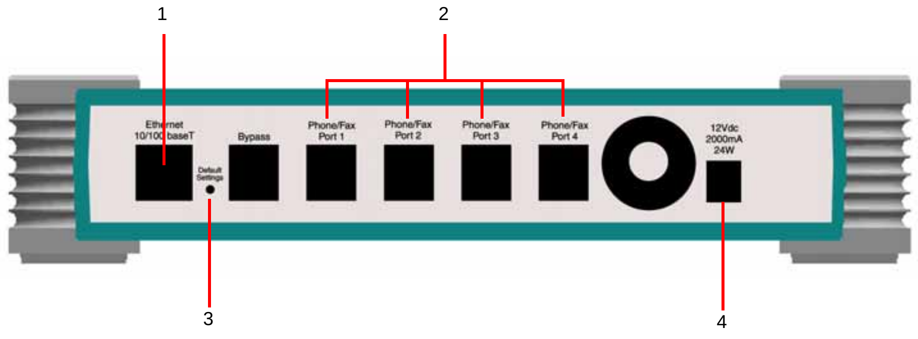
1. Connect a 10/100 BaseT Ethernet RJ-45 cable into the *Ethernet* connector of the HiPath AP 1140 and connect the other end to the network.
2. Connect analog telephones or fax machines to Ports 1, 2, 3, and 4.
3. Connect a SCN line into the *Bypass* port of the HiPath AP 1140 (optional).

   In case of power failure or down network conditions, this SCN line will be connected to the telephone on Port 1 and you will be able to use the phone. For more information, see “System Failure Bypass Activation Section” on page 68.
4. Connect the power supply to the HiPath AP 1140 and then connect the power cable to an electrical outlet.

!	The electrical outlet shall be installed near the HiPath AP 1140 so that it is easily accessible.

ℹ	If you are installing the HiPath AP 1140 for the first time, please read section “Setting up the HiPath AP 1140 for the First Time” on page 10 before proceeding.

Figure 5: Hardware Installation Steps



Basic Configuration

The HiPath AP 1140 application contains **a**n embedded web server to access its configuration web pages by using an Internet browser. This chapter describes how to access and use the configuration web pages to set parameters using the HTTP protocol.

Web Interface

To properly access the web interface, your Web browser must support:

- Frames
- HTML 4.0

Suitable Web browsers are:

- Netscape® Navigator™ Version 4.7 or above
- Microsoft® Internet Explorer Version 5.0 or above

Accessing the Web Interface

The web interface gives you an overview of the HiPath AP 1140 parameters.

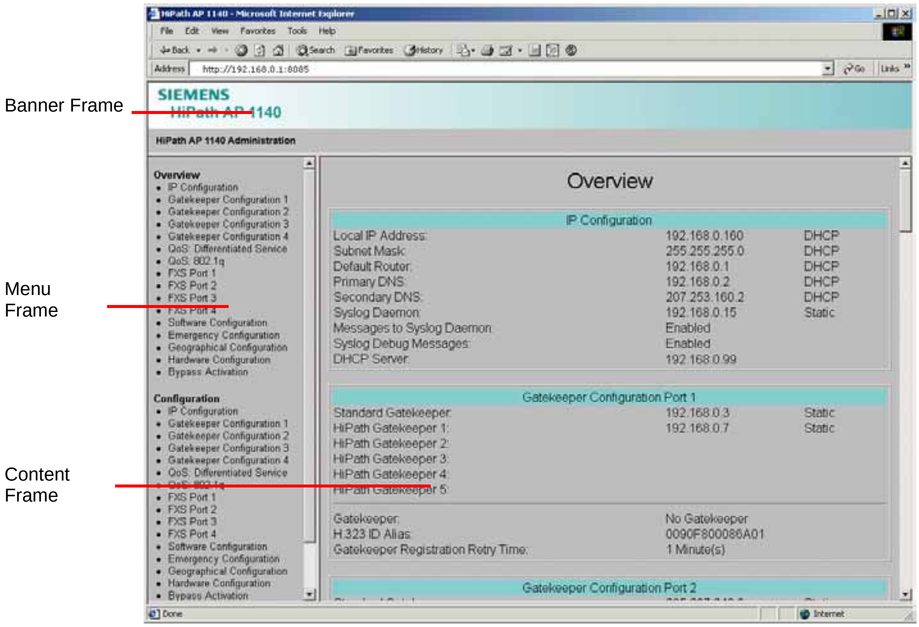
▶ **To access the configuration web pages:**

1. In your web browser’s address field, type the URL of the HiPath AP 1140.

   This must be in the format:
   `http://nnn.nnn.nnn.nnn:8085`

   where ***nnn.nnn.nnn.nnn*** is the IP address of the HiPath AP 1140 and ***:8085*** is the web server port. For example, if the IP address of your HiPath AP 1140 is *192.168.0.94*, type it in your web browser’s address field followed by *:8085*. If you are using the HiPath AP 1140 for the first time, use the default IP address *192.168.0.1*. The following will appear:

Figure 6: Configuration Web Pages


Banner Frame
Menu Frame
Content Frame
HiPath AP 1140 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.0.1:8085
Go Links
SIEMENS
HiPath AP 1140
HiPath AP 1140 Administration
Overview
IP Configuration
Gatekeeper Configuration 1
Gatekeeper Configuration 2
Gatekeeper Configuration 3
Gatekeeper Configuration 4
QoS: Differentiated Service
QoS: 802.1q
FXS Port 1
FXS Port 2
FXS Port 3
FXS Port 4
Software Configuration
Emergency Configuration
Geographical Configuration
Hardware Configuration
Bypass Activation
Configuration
IP Configuration
Gatekeeper Configuration 1
Gatekeeper Configuration 2
Gatekeeper Configuration 3
Gatekeeper Configuration 4
QoS: Differentiated Service
QoS: 802.1q
FXS Port 1
FXS Port 2
FXS Port 3
FXS Port 4
Software Configuration
Emergency Configuration
Geographical Configuration
Hardware Configuration
Bypass Activation
Done
Internet

Overview

IP Configuration		
Local IP Address:	192.168.0.160	DHCP
Subnet Mask:	255.255.255.0	DHCP
Default Router:	192.168.0.1	DHCP
Primary DNS:	192.168.0.2	DHCP
Secondary DNS:	207.253.160.2	DHCP
Syslog Daemon:	192.168.0.15	Static
Messages to Syslog Daemon:	Enabled	
Syslog Debug Messages:	Enabled	
DHCP Server:	192.168.0.99	

Gatekeeper Configuration Port 1		
Standard Gatekeeper:	192.168.0.3	Static
HiPath Gatekeeper 1:	192.168.0.7	Static
HiPath Gatekeeper 2:		
HiPath Gatekeeper 3:		
HiPath Gatekeeper 4:		
HiPath Gatekeeper 5:		
Gatekeeper:	No Gatekeeper	
H.323 ID Alias:	0090F800086A01	
Gatekeeper Registration Retry Time:	1 Minute(s)	

Gatekeeper Configuration Port 2

The Banner Frame

This is at the top of the browser window.

The Menu Frame

The Menu frame is displayed down the left side of the browser window. It contains management links that allow you to display web pages in the Content frame.

Link	Description
Overview	Links to the *Overview* web page, which displays the parameters and IP addresses used by the HiPath AP 1140 in read-only format.
Configuration	Links to the *Configuration* web page, which allows you to set the parameters and IP addresses used by the HiPath AP 1140.
Change Password	Links to the *Change Password/User Name* web page, which allows you to change your own password and user name.

Link	Description
Advanced Debug	Links to the *Advanced Debug page*, which produces output for debugging, monitoring and tracking the HiPath AP 1140 application.

The Content Frame

The Content frame is displayed in the lower right part of the browser window. It contains the various web pages that allow you to manage the HiPath AP 1140.

Accessing the Configuration Web Page

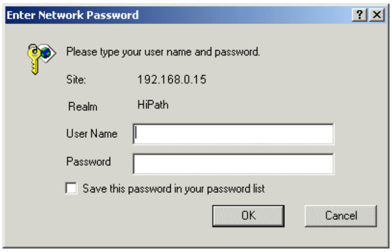
The *Configuration* page allows you to set the parameters of the HiPath AP 1140.

▶ **To access the *Configuration* page:**

1. Click the *Configuration* link of the menu frame.

   If you are accessing the configuration pages for the first time, the following dialog box opens:

   Figure 7: Enter Network Password Window

   Please type your user name and password.

   Site: 192.168.0.15

   Realm HiPath

2. Enter the proper user name and password in this dialog.

   The user name and password must be valid. They are case sensitive hence they must be entered properly. Default values are:

   – **User Name**: HiPathAdm

   – **Password**: 8749Trix

3. Click *OK*.

   The *Configuration* web page is then displayed in the content frame. It stays accessible for as long as the Internet browser used to access the HiPath AP 1140 web pages is opened.

Using the Configuration Buttons

The following table lists the buttons you can use to manage the HiPath AP 1140. These buttons are located at the bottom of the web browser.

ℹ To make these buttons visible, you must click one of the links of the *Configuration* section (in the Menu frame).

Button	Description
Update	Updates the HiPath AP 1140 configuration with the changes you have made. See “Updating the Configuration” on page 21 for more details.
Download	Starts a new software download. See “Setting up Software Download” on page 83 for more details.
Restart	Restarts the HiPath AP 1140 unit. See “Restarting the HiPath AP 1140” on page 22 for more details.
Reset	Resets the fields of the *Configuration* web page to their previous values. See “Resetting the Configuration” on page 22 for more details.
Static IP	Checks all the Static checkboxes in one operation, instead of checking them one by one. **Note**: When all IP addresses are static, there is no DHCP request.
DHCP IP	Clears all the Static checkboxes in one operation, instead of unchecking them one by one. The IP addresses in the Static/DHCP failure fields are not deleted.
RAM Check	Starts a RAM check process. See “Performing a RAM Check” on page 67 for more details.
ROM Check	Starts a ROM check process. See “Performing a ROM Check” on page 68 for more details.

Updating the Configuration

▶ **To make changes to the *Configuration* page:**

1. Set the parameters you want to change/update.

You can click *Reset* at any time to reset the parameters to the previous values.

2. Click *Update* to apply the changes.

The HiPath AP 1140 configuration is updated with the values in the *Configuration* web page fields (this will take 10 to 20 seconds).

Most changes will automatically restart the HiPath AP 1140 after clicking the *Update* button. If one of the modified fields contains an error, a message is displayed and the configuration update is not processed.

If the HiPath AP 1140 is in use at the same time you click *Update*, the configuration update is not processed. A message informs you of this situation.

The reverse situation is also true. For example, if the user tries to use an FXS port while the HiPath AP 1140 processes a configuration update, the telephone handset sends a busy tone and no call can be made nor received.

If the HiPath AP 1140 is not in use at the same time you click *Update*, the configuration update is processed.

3. Refresh the web page.

The new changes are displayed and in effect.

Please note that some settings are automatically effective and will not require the HiPath AP 1140 to reboot if you **only** change their values. These settings are:

- *Software Download Configuration* section
- *Emergency Software Configuration* section
- *Call Forward* settings of the *Port* section.
- *Messages to Syslog Daemon* check box in the *IP Configuration* section
- *Syslog Debug Messages* check box in the *IP Configuration* section.

Restarting the HiPath AP 1140

Clicking on the *Restart* button at the bottom of the *Configuration* web page restarts the HiPath AP 1140. If the unit is in use when you click *Restart*, the restart is not processed. A message informs you of this situation.

If the HiPath AP 1140 is not in use when you click *Restart*, a message informs you that the unit is about to restart. Approximately 10 to 20 seconds after receiving this message, you can request the HiPath AP 1140 web pages.

Resetting the Configuration

You can delete all changes made in the *Configuration* web page field by clicking the *Reset* button at the bottom of the *Configuration* web page. The HiPath AP 1140 configuration is not updated. The *Configuration* web page is refreshed with the values of the actual parameters and IP addresses of the HiPath AP 1140.

Integrating the HiPath AP 1140 into the Communication Environment

The HiPath AP 1140 is managed as a terminal unit within an individual LAN and it must have an IP address like any other unit connected. It can operate both within a HiPath environment (version 3.0) and without a HiPath environment. If you have any questions about the individual terms used or about your LAN environment, please contact your network administrator.

The HiPath AP 1140 can be configured to receive an IP address automatically from the DHCP server as soon as it is connected to a LAN, or to use static IP addresses you have defined.

The HiPath AP 1140 uses other IP addresses as well, such as gatekeeper IP addresses. These addresses can also be assigned via DHCP server or defined manually.

The following sections of the *Configuration* web page use IP addresses:

– IP Configuration

Network Management

When managing an HiPath AP 1140 over the network, the unit must be correctly configured with an IP address and a subnet mask.

IP Addresses

To operate correctly, each unit on a network must have a unique IP address. IP addresses have the format *n.n.n.n* where *n* is a decimal number between 0 and 255, for example, *192.168.0.1*. If your network has a connection to the external IP network, you need to apply for a registered IP address. This system ensures that each IP address is unique; if you do not have a registered IP address, you may be using an address identical to someone else’s and your network may not operate correctly.

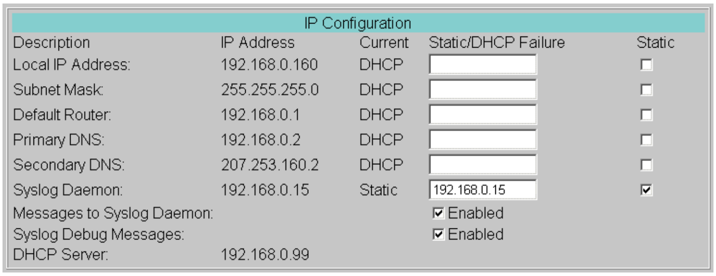
Subnets and Using a Subnet Mask

You can divide your IP network into sub-networks or subnets. Support for subnets is important because the number of bits assigned to the device part of an IP address limits the number of devices that may be addressed on any given network. For example, a Class C address is restricted to 254 devices. Note that if you have a small network (less than 254 devices), you may decide not to have subnets.

If you are unsure about what mask to use, Siemens AG suggests that you use a general mask, *255.255.255.0*.

- Gatekeeper Configuration
- Software Download Configuration
- Emergency Software Configuration

Figure 8: Example – IP Configuration Section



IP Configuration

Description	IP Address	Current	Static/DHCP Failure	Static
Local IP Address:	192.168.0.160	DHCP		☐
Subnet Mask:	255.255.255.0	DHCP		☐
Default Router:	192.168.0.1	DHCP		☐
Primary DNS:	192.168.0.2	DHCP		☐
Secondary DNS:	207.253.160.2	DHCP		☐
Syslog Daemon:	192.168.0.15	Static	192.168.0.15	☑
Messages to Syslog Daemon:			☑ Enabled	
Syslog Debug Messages:			☑ Enabled	
DHCP Server:	192.168.0.99			

The IP information is broken down into five columns:

Column	Description
Description	Brief description of the IP address.
IP address	Actual IP address.

Column	Description
Current	Source of the IP address. – *DHCP*: A DHCP server provided the IP address when the HiPath AP 1140 was powered on. – *Static*: You checked the *Static* checkbox and manually specified a static IP address in the *Static/DHCP failure* field. This IP address overrides the corresponding IP address provided by a DHCP server (if applicable). The *Current* field can be empty in the following two situations: – The *IP address* field and the *Static/DHCP failure* field have the same IP address. There was no DHCP server available to provide an IP address so the IP address of the *Static/DHCP failure* field is actually used. Note that in this case, the *Static* checkbox is NOT checked. – There is no IP address in the *Static/DHCP failure* field. There was no DHCP server available to provide an IP address and there was no IP address in the *Static/DHCP failure* field. The IP address used in this case is the one in the last successfully saved configuration. This IP address might be an IP address previously provided by a DHCP server or specified in the *Static/DHCP failure* field.
Static/DHCP failure	Used to manually specify an IP address. **Note**: If there is an IP address in this field, but the *Static* option is not checked, the DHCP server settings will override the static settings. In the event that the HiPath AP 1140's IP address is configured statically (*Static* check box is checked), you should reserve the specified IP address in the DHCP server to ensure that it does not assign the HiPath AP 1140 IP address to another device.

Column	Description
Static	Indicates whether the IP address in the *Static/DHCP failure* field is used or if the corresponding IP address provided by a DHCP server is used. If the *Static* checkbox is checked, the IP address in the *Static/DHCP failure* field is always used instead of the corresponding IP address provided by a DHCP server. **Note**: When all IP addresses are static, there is no DHCP request. If the *Static* checkbox is NOT checked, the IP address in the *Static/DHCP failure* field is used only if no DHCP server could provide the corresponding IP address. If the row of an IP address is empty, it means one of the following: – No static value was specified for this IP address (in the *Static/DHCP failure* field with the *Static* checkbox checked). – No DHCP server could provide an IP address the last time the HiPath AP 1140 was powered on. – No rescue value was given for this IP address (in the *Static/DHCP failure* field with the *Static* checkbox NOT checked). – No IP address was found in the last good saved configuration of the HiPath AP 1140.

All of the IP addresses provided by a DHCP server are saved in the HiPath AP 1140 configuration, even if they are not actually used. When powered on, the HiPath AP 1140 uses the IP addresses saved in its configuration and/or the IP addresses provided by a DHCP server.

If the *Static* checkbox is NOT checked, the HiPath AP 1140 uses an IP address in the following order:

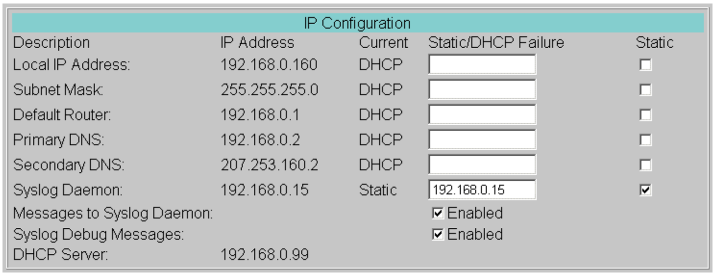
1. IP address provided by a DHCP server.
2. If no DHCP server provides the IP address, IP address from the *Static/DHCP failure* field.
3. If the *Static/DHCP failure* field is empty, an IP address from the last good saved configuration.
4. If no IP address was previously saved in the configuration, there is no valid IP address value.

When the *Static* option is checked, the HiPath AP 1140 uses the IP address in the corresponding *Static/DHCP failure* field.

Configuring IP Addresses

The *IP Configuration* section sets the general IP addresses used by the HiPath AP 1140.

Figure 9: IP Configuration Section



IP Configuration

Description	IP Address	Current	Static/DHCP Failure	Static
Local IP Address:	192.168.0.160	DHCP		☐
Subnet Mask:	255.255.255.0	DHCP		☐
Default Router:	192.168.0.1	DHCP		☐
Primary DNS:	192.168.0.2	DHCP		☐
Secondary DNS:	207.253.160.2	DHCP		☐
Syslog Daemon:	192.168.0.15	Static	192.168.0.15	☑
Messages to Syslog Daemon:			☑ Enabled	
Syslog Debug Messages:			☑ Enabled	
DHCP Server:	192.168.0.99			

The following table describes the parameters that can be set:

Parameter	Definition
Local IP Address	IP address of the HiPath AP 1140.
Subnet Mask	Subnet mask IP address used by the HiPath AP 1140. The subnet mask enables the network administrator to further divide the host part of the address into two or more subnets.
Default Router	Default router IP address used by the HiPath AP 1140. A router is a device that connects any number of LANs.
Primary DNS	Primary Domain Name Server IP address used by the HiPath AP 1140. A DNS is an Internet service that translates domain names into IP addresses.
Secondary DNS	Secondary Domain Name Server IP address used by the HiPath AP 1140. A DNS is an Internet service that translates domain names into IP addresses.

Parameter	**Definition**
Syslog Daemon	IP address of the server running a Syslog daemon.The Syslog Daemon allows you to monitor events in a HiPath AP 1140. If you do not specify a Syslog daemon address or the DHCP does not provide one, no messages are sent. **Note**: See "Appendix A – DHCP Server Vendor Specific Information" on page 95 for more details.
Messages to Syslog Daemon	When the *Enabled* option is checked and a *Syslog daemon* IP address is specified, messages are sent to the Syslog daemon. When the *Enabled* option is not checked, no messages are sent to the Syslog daemon.
Syslog Debug Messages	When the *Enabled* option is checked, the HiPath AP 1140 sends Syslog messages of debug type. **Note**: This option should be used only for troubleshooting major problems, because it generates a lot of messages. If many HiPath AP 1140 units are configured to send Syslog debug messages, it could create an unnecessary burden on the network traffic.
DHCP Server	IP address of the DHCP server used by the HiPath AP 1140. If no DHCP server is available, no IP address is displayed. This information is read-only.

Using a Syslog Daemon

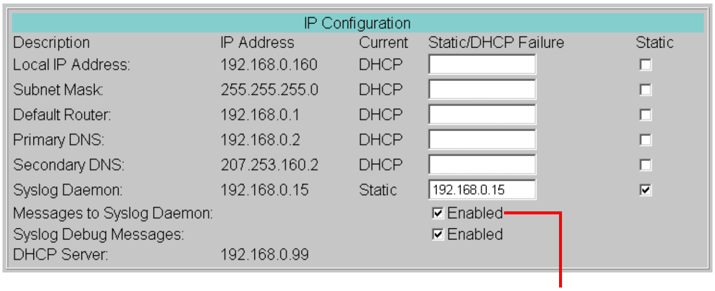
The Syslog daemon is a general purpose utility for monitoring applications and network devices with the TCP/IP protocol. With this software, you can monitor useful messages coming from your HiPath AP 1140 unit.

For instance, if you want to download a new software into your HiPath AP 1140, you can monitor each step of the software download process. Furthermore, if your HiPath AP 1140 encounters an abnormal behaviour, you may see accurate messages that will help you troubleshoot the problem.

▶ **To configure the HiPath AP 1140 to send Syslog messages:**

1. In the *Configuration* page, go to the *IP Configuration* section and enter the IP address of the server running the Syslog daemon. Make sure that you check the *Static* option on the right.
2. Enable *Messages to Syslog Daemon*.

Figure 10: Syslog Daemon



IP Configuration

Description	IP Address	Current	Static/DHCP Failure	Static
Local IP Address:	192.168.0.160	DHCP		☐
Subnet Mask:	255.255.255.0	DHCP		☐
Default Router:	192.168.0.1	DHCP		☐
Primary DNS:	192.168.0.2	DHCP		☐
Secondary DNS:	207.253.160.2	DHCP		☐
Syslog Daemon:	192.168.0.15	Static	192.168.0.15	☑
Messages to Syslog Daemon:			☑ Enabled	
Syslog Debug Messages:			☑ Enabled	
DHCP Server:	192.168.0.99			

Click here to enable messages to the Syslog daemon

3. Click *Update* to apply the changes.

   The HiPath AP 1140 restarts. You can now use the Syslog daemon to receive messages from the HiPath AP 1140.

Changing the Password/User Name

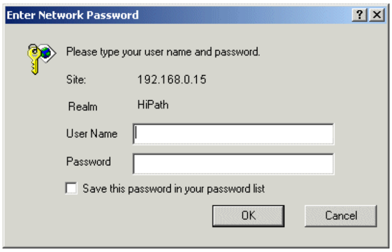
A default user name and password are provided with the HiPath AP 1140. However, you can use your own set of user name and password.

▶ **To access the *Change Password/User Name* page:**

1. Click the *Change Password* link of the Menu frame.

   If you are accessing the configuration pages for the first time, the following dialog box opens:

Figure 11: Enter Network Password Window



Enter Network Password

Please type your user name and password.

Site: 192.168.0.15

Realm HiPath

User Name

Password

☐ Save this password in your password list

2. Enter the default user name and password.

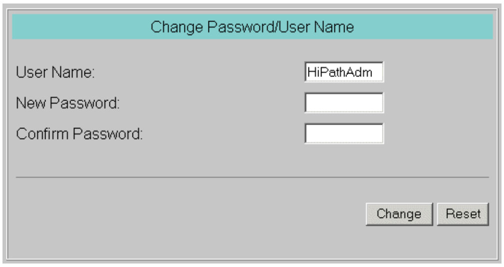
The user name and password must be valid. The user name and password are case sensitive hence they must be entered properly.The default values are:

- **User Name:** HiPathAdm
- **Password:** 8749Trix

3. Click *OK*.

The *Change Password/User Name* web page is displayed in the content frame and it stays accessible for as long as the Internet browser used to access the HiPath AP 1140 web pages is opened.

Figure 12: Change Password/User Name Web Page



Change Password/User Name

User Name: HiPathAdm

New Password:

Confirm Password:

▶ **To change the current user name and password:**

1. Enter your new user name and password.

2. Retype your password in the *Confirm Password* field.

3. Click *Change*.

The following table describes the parameters that can be changed:

Parameter	Definition
User name	User name used in the login process. It is case sensitive. **Value:** A string of 6 to 10 alphanumeric characters (a-z, A-Z, 0-9). The user name must not contain spaces. **Default value:** HiPathAdm
Password	Password used in the login process. It is case sensitive. **Value:** A string of 6 to 10 alphanumeric characters (a-z, A-Z, 0-9). The password must not contain spaces. **Default value:** 8749Trix

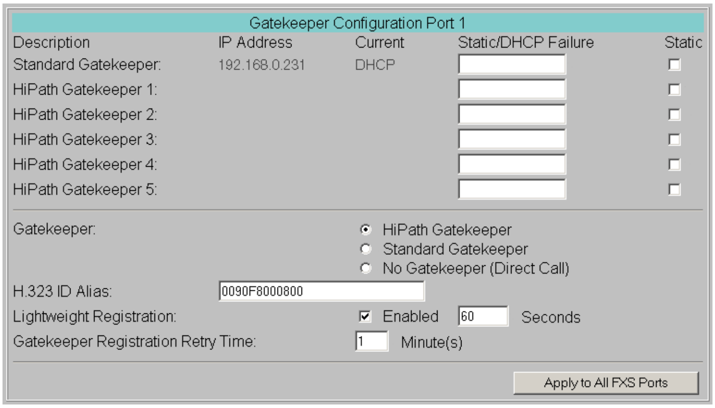
Registering to a Gatekeeper

This chapter describes how to configure each FXS port of your HiPath AP 1140 to register to a gatekeeper. Each FXS port of the HiPath AP 1140 registers to a gatekeeper individualy and can be configured with different settings.

Setting up Gatekeeper Information

If a FXS port is configured to register to a gatekeeper (*HiPath Gatekeeper* or *Standard Gatekeeper*), direct calls are not allowed, even if there is no IP address(es) for a gatekeeper. Direct calls are made by dialing an IP address and are allowed only if the FXS port is not configured to register to a gatekeeper.

Figure 13: Gatekeeper Configuration Section



Gatekeeper Configuration Port 1

Description	IP Address	Current	Static/DHCP Failure	Static
Standard Gatekeeper:	192.168.0.231	DHCP		☐
HiPath Gatekeeper 1:				☐
HiPath Gatekeeper 2:				☐
HiPath Gatekeeper 3:				☐
HiPath Gatekeeper 4:				☐
HiPath Gatekeeper 5:				☐

Gatekeeper: ● HiPath Gatekeeper ○ Standard Gatekeeper ○ No Gatekeeper (Direct Call)

H.323 ID Alias: 0090F8000800

Lightweight Registration: ☑ Enabled 60 Seconds

Gatekeeper Registration Retry Time: 1 Minute(s)

All parameters can be identical for each FXS port. If this is what you want, click *Apply to All FXS Ports* in the *Gatekeeper Configuration Port 1* section once the parameters are set. The parameters will be applied to all four FXS ports.

If you want to assign different values to each FXS port, you can do so by setting the corresponding *Gatekeeper Configuration Port* sections.

The following table describes the parameters that can be set:

Parameter	Definition
Standard Gatekeeper	IP address of a standard gatekeeper used during the gatekeeper registration process. See "Gatekeeper Registration Logic" on page 35 for more details.

Parameter	Definition
HiPath Gatekeeper addresses	IP addresses of HiPath gatekeepers used during the HiPath gatekeeper registration process. If the HiPath gatekeeper registration fails with the first HiPath gatekeeper, the HiPath AP 1140 tries to register to the second HiPath gatekeeper and so on. The IP address of at least one HiPath gatekeeper must be specified. The IP addresses of up to five HiPath gatekeepers can be specified. See "Gatekeeper Registration Logic" on page 35 for more details.
Gatekeeper	Type of gatekeeper to register to. Please note that *No Gatekeeper* is the only mode where direct calls are allowed. See "Gatekeeper Registration Logic" on page 35 for more details. **Values**: HiPath Gatekeeper, Standard Gatekeeper, No Gatekeeper **Note**: If you select the HiPath Gatekeeper type, the autodiscovery feature of the HiPath 5000 system will overwrite any value entered in the DiffServ field of the HiPath AP 1140. See "Differentiated Services (DiffServ) Section" on page 56 for more details. **Default**: HiPath Gatekeeper
H.323 ID Alias	H.323 ID alias used in the gatekeeper registration process. If the selected type of gatekeeper is *HiPath Gatekeeper*, the value of this field must be the same as the login ID of the HiPath gatekeeper subscriber associated with the FXS port. A H.323 ID may look like a telephone number but this is not the recommendation. If the selected type of gatekeeper is *Standard Gatekeeper*, it is up to the gatekeeper administrator to attribute the value of the H.323 ID alias to the FXS port. **Value:** A string of up to 50 alphanumeric characters (a-z, A-Z, 0-9). Spaces are allowed. **Default value**: The MAC address of the HiPath AP 1140 plus "0" plus the FXS port number. For example, if the MAC address of a HiPath AP 1140 is 0498B8000ABC, the default H.323 ID alias of the FXS port 1 will be 0498B8000ABC01.The default H.323 ID alias of the FXS port 2 will be 0498B8000ABC02, and so on.

Parameter	Definition
Lightweight Registration	The lightweight registration mechanism is used to verify the sanity of the gatekeeper. It allows the HiPath AP 1140 to verify if the gatekeeper is still "alive". When the "Lightweight Registration" option is enabled and once the HiPath AP 1140 is registered, it "re-registers" to the gatekeeper at a specific interval. This interval is in seconds and is the value of the "Lightweight Registration" option. If the gatekeeper does not respond to one of these re-registration requests, the HiPath AP 1140 knows that the gatekeeper is not functional. The HiPath AP 1140 then tries to register again. See "Lightweight Registration" on page 39 for more details.
Gatekeeper Registration Retry Time	The number of minutes the FXS port waits before trying to register again. See "Gatekeeper Registration Logic" on page 35 for more details. **Value**: Any number of minutes between 1 and 60. **Default value**: 1

For the IP addresses in this section, refer to " Appendix A – DHCP Server Vendor Specific Information" on page 95 for DHCP server vendor-specific information.

Gatekeeper Registration Logic

This section describes the gatekeeper registration process of the HiPath AP 1140.

Each FXS port of the HiPath AP 1140 registers individualy. The FXS ports can register to the same gatekeeper or to a different gatekeeper. Some FXS ports can be configured to register to a gatekeeper while the other FXS ports are not configured to register to a gatekeeper.

To simplify the examples that follow, reference is made to the HiPath AP 1140 in general. But these examples really apply to each FXS port.

No Gatekeeper Registration

When the *Gatekeeper* field is equal to *No gatekeeper (direct call)* (see "Setting up Gatekeeper Information" on page 33), the HiPath AP 1140 does not send a gatekeeper registration request. The value of the *Retry time* field is useless. The HiPath AP 1140 can make or receive calls to/from other unregistered H.323 endpoints. Some gatekeepers allow a registered H.323 endpoint to call an unregistered H.323 endpoint and vice versa. This issue is gatekeeper-dependent and is not addressed here.

Messages Exchanged

The following section describes the messages exchanged between a HiPath AP 1140 and a gatekeeper.

▶ **When a HiPath AP 1140 wants to register to a gatekeeper:**

- The HiPath AP 1140 sends a **registration request** message to the gatekeeper.
- If the gatekeeper accepts the registration request from the HiPath AP 1140, it replies with a **registration confirm** message.
- If the gatekeeper refuses the registration request from the HiPath AP 1140, it replies with a **registration reject** message.

▶ **When a gatekeeper wants to terminate the registration of a HiPath AP 1140:**

- The gatekeeper sends an **unregistration request** message to the HiPath AP 1140.
- If the HiPath AP 1140 accepts the unregistration request from the gatekeeper, it replies with an **unregistration confirm** message.
- If the HiPath AP 1140 refuses the unregistration request from the gatekeeper, it replies with an **unregistration reject** message.

▶ **When a HiPath AP 1140 is registered and it wants to make a call:**

- The HiPath AP 1140 sends an **admission request** message to the gatekeeper.

  The HiPath AP 1140 asks the gatekeeper the permission to make a call.
- If the gatekeeper gives the permission to make the call, it replies with an **admission confirm** message.
- If the gatekeeper refuses to give the permission to make the call, it replies with an **admission reject** message.

Registration to a Gatekeeper

When the *Gatekeeper* field is equal to *HiPath gatekeeper* or *Standard gatekeeper* (see "Setting up Gatekeeper Information" on page 33), the HiPath AP 1140 **can't** make or receive calls as long as it is not registered. If the user picks up the telephone handset while the HiPath AP 1140 is trying to register, a special tone is played. This special tone is a pulsed busy tone with a 5 seconds *busy tone*/*no tone* cycle.

The value in the *Retry time* field is the number of minutes the HiPath AP 1140 waits before trying to register again. This value is used only after the second gatekeeper registration request.

The following states describe the gatekeeper registration logic of the HiPath AP 1140.

State	Comments
State 1: HiPath AP 1140 tries to register to the gatekeeper a first time.	– If the registration is successful, the gatekeeper registration is completed. The HiPath AP 1140 enters state 5. – If the gatekeeper does not reply to the registration request of the HiPath AP 1140, the registration request times out. The HiPath AP 1140 enters state 2. – If the gatekeeper rejects the registration request of the HiPath AP 1140, the HiPath AP 1140 enters state 2.
State 2: The HiPath AP 1140 tries to register to the gatekeeper a second time.	– If the registration is successful, the gatekeeper registration is completed. The HiPath AP 1140 enters state 5. – If the gatekeeper does not reply to the registration request of the HiPath AP 1140, the registration request times out. The HiPath AP 1140 enters state 3. – If the gatekeeper rejects the registration request of the HiPath AP 1140, the HiPath AP 1140 enters state 3.

State	Comments
State 3: The HiPath AP 1140 waits a certain number of minutes before retrying to register.	– The number of minutes is defined in the *Retry time* field. Once the waiting period is over, the HiPath AP 1140 enters state 4.
State 4: The HiPath AP 1140 tries to register to the gatekeeper.	– If the registration is successful, the gatekeeper registration is completed. The HiPath AP 1140 enters state 5. – If the gatekeeper does not reply to the registration request of the HiPath AP 1140, the registration request times out. The HiPath AP 1140 enters state 3. – If the gatekeeper rejects the registration request of the HiPath AP 1140, the HiPath AP 1140 enters state 3.
State 5: The HiPath AP 1140 is registered.	

Note about states 1, 2 and 4

If the HiPath AP 1140 is configured with the IP addresses of many gatekeepers, it tries to register to each IP address before entering the next state. For instance, a HiPath AP 1140 is configured with the IP addresses of five HiPath gatekeepers, *HiPath gatekeeper 1* to *HiPath gatekeeper 5*. The HiPath AP 1140 enters state 1 and:

1. The HiPath AP 1140 tries to register to *HiPath gatekeeper 1*. The registration request times out or is rejected by *HiPath gatekeeper 1*. The HiPath AP 1140 **does not** enter state 2.
2. The HiPath AP 1140 tries to register to *HiPath gatekeeper 2*. The registration request times out or is rejected by *HiPath gatekeeper 2*. The HiPath AP 1140 **does not** enter state 2.
3. The HiPath AP 1140 tries to register to *HiPath gatekeeper 3*. The registration request times out or is rejected by *HiPath gatekeeper 3*. The HiPath AP 1140 **does not** enter state 2.

4. The HiPath AP 1140 tries to register to *HiPath gatekeeper 4*. The registration request times out or is rejected by *HiPath gatekeeper 4*. The HiPath AP 1140 **does not** enter state 2.
5. The HiPath AP 1140 tries to register to *HiPath gatekeeper 5*. The registration request times out or is rejected by *HiPath gatekeeper 5*. **Now the HiPath AP 1140 enters state 2.**

Lightweight Registration

The lightweight registration mechanism allows the HiPath AP 1140 to verify if the gatekeeper is still "alive". See “Setting up Gatekeeper Information” on page 33 for more details.

▶ **If the "Lightweight Registration" option is enabled:**

- The *timeToLive* field is included in the registration request messages.
- The *timeToLive* field is set to the value of the "Lightweight Registration" option.
- If the gatekeeper sends a registration confirm message without a *timeToLive* field, the HiPath AP 1140 does not send lightweight registration request messages.
- If the gatekeeper sends a registration confirm message with a *timeToLive* field, the HiPath AP 1140 sends a lightweight registration request message at a steady interval. This interval is equal to one-third the value of the *timeToLive* field from the registration confirm message.

▶ **If the gatekeeper does not respond to a lightweight registration request message (if a lightweight registration message times out):**

1. The HiPath AP 1140 sends another lightweight registration message.
2. If the gatekeeper still does not respond, the HiPath AP 1140 waits 60 seconds.
3. Steps 1 and 2 are repeated 4 times. After the fourth lightweight registration message times out, the HiPath AP 1140 starts its registration process from the beginning (as if it had just rebooted).

▶ **If the "Lightweight Registration" option is disabled:**

- The *timeToLive* field is not included in the registration request messages.
- The HiPath AP 1140 does not send lightweight registration request messages.

- Even if the gatekeeper returns a registration confirm message containing a *timeToLive* field, the HiPath AP 1140 does not send lightweight registration request messages.

Examples

The following are examples that illustrate the gatekeeper registration logic.

Registering to a Standard Gatekeeper

There is an electric shortage. After a few minutes, the power comes back. The HiPath AP 1140 and the standard gatekeeper reboot. The HiPath AP 1140 reboots faster than the standard gatekeeper does. The value of the *Retry time* is set to 1 minute.

1. The HiPath AP 1140 tries to register a first time to the standard gatekeeper but the registration request times out. The standard gatekeeper is not ready.
2. The HiPath AP 1140 tries to register a second time to the standard gatekeeper but the registration request times out. The standard gatekeeper is not ready.
3. The HiPath AP 1140 waits one (1) minute without trying to register.
4. The HiPath AP 1140 tries to register to the standard gatekeeper but the registration request times out. The standard gatekeeper is still not ready.
5. The HiPath AP 1140 waits one (1) minute without trying to register.
6. The HiPath AP 1140 tries to register to the standard gatekeeper. The standard gatekeeper is now ready. The HiPath AP 1140 is now registered to the standard gatekeeper.

Registering to a List of Five HiPath Gatekeepers

There are five (5) HiPath gatekeepers, HiPath gatekeepers 1 to 5. They are configured to accept the registration requests from the HiPath AP 1140.

There is an electric shortage. After a few minutes, the power comes back. The HiPath AP 1140 and the HiPath gatekeepers reboot. The HiPath AP 1140 reboots faster than the HiPath gatekeepers do. The value of the *Retry time* field is set to 5 minutes.

1. The HiPath AP 1140 tries to register a first time to *HiPath gatekeeper 1* but the registration request times out. *HiPath gatekeeper 1* is not ready.

2. The HiPath AP 1140 tries to register a first time to *HiPath gatekeeper 2* but the registration request times out. *HiPath gatekeeper 2* is not ready.
3. The HiPath AP 1140 tries to register a first time to *HiPath gatekeeper 3* but the registration request times out. *HiPath gatekeeper 3* is not ready.
4. The HiPath AP 1140 tries to register a first time to *HiPath gatekeeper 4* but the registration request times out. *HiPath gatekeeper 4* is not ready.
5. The HiPath AP 1140 tries to register a first time to *HiPath gatekeeper 5* but the registration request times out. *HiPath gatekeeper 5* is not ready.
6. The HiPath AP 1140 tries to register a second time to *HiPath gatekeeper 1* but the registration request times out. *HiPath gatekeeper 1* is still not ready.
7. The HiPath AP 1140 tries to register a second time to *HiPath gatekeeper 2* but the registration request times out. *HiPath gatekeeper 2* is still not ready.
8. The HiPath AP 1140 tries to register a second time to *HiPath gatekeeper 3* but the registration request times out. *HiPath gatekeeper 3* is still not ready.
9. The HiPath AP 1140 tries to register a second time to *HiPath gatekeeper 4* but the registration request times out. *HiPath gatekeeper 4* is still not ready.
10. The HiPath AP 1140 tries to register a second time to *HiPath gatekeeper 5* but the registration request times out. *HiPath gatekeeper 5* is still not ready.
11. The HiPath AP 1140 waits five (5) minutes without trying to register.
12. The HiPath AP 1140 tries to register to *HiPath gatekeeper 1* but the registration request times out. *HiPath gatekeeper 1* is still not ready.
13. The HiPath AP 1140 tries to register to *HiPath gatekeeper 2*. *HiPath gatekeeper 2* is now ready. The HiPath AP 1140 is registered to *HiPath gatekeeper 2*.

Registration Reject from a HiPath Gatekeeper

There are three HiPath gatekeepers, *HiPath gatekeepers* 1 to 3. Only *HiPath gatekeeper 3* is configured to accept the registration requests from the HiPath AP 1140.

In this example, you change the value of the *Voice coding algorithm* field (see “Configuring Incoming and Outgoing Calls Parameters” on page 45) and click *Update* in order to update the configuration of the HiPath AP 1140. The HiPath AP 1140 resets and starts its gatekeeper registration. The value of the *Retry time* field is set to 3 minutes.

1. The HiPath AP 1140 tries to register to *HiPath gatekeeper 1*, which rejects the registration request from the HiPath AP 1140. *HiPath gatekeeper 1* is not configured to accept the registration requests from the HiPath AP 1140.
2. The HiPath AP 1140 tries to register to *HiPath gatekeeper 2*, which rejects the registration request from the HiPath AP 1140. *HiPath gatekeeper 2* is not configured to accept the registration requests from the HiPath AP 1140.
3. The HiPath AP 1140 tries to register to *HiPath gatekeeper 3*, which accepts the registration request from the HiPath AP 1140. The HiPath AP 1140 is now registered to *HiPath gatekeeper 3*.

Unregistration Request from a HiPath Gatekeeper

There is only one HiPath gatekeeper, *HiPath gatekeeper 1*. It is configured to accept the registration requests from the HiPath AP 1140. The value of the *Retry time* field is set to 3 minutes.

1. The HiPath AP 1140 is registered to *HiPath gatekeeper 1*.
2. *HiPath gatekeeper 1* must be reset for maintenance purposes. It sends the unregistration request message to the HiPath AP 1140.
3. The HiPath AP 1140 receives the unregistration request message and replies with the unregistration confirm message. The HiPath AP 1140 is not registered to *HiPath gatekeeper 1* anymore.
4. The HiPath AP 1140 waits three (3) minutes without trying to register.
5. The HiPath AP 1140 tries to register to *HiPath gatekeeper 1* but the registration request times out. *HiPath gatekeeper 1* is not ready.
6. The HiPath AP 1140 waits three (3) minutes without trying to register.

7. The HiPath AP 1140 tries to register to *HiPath gatekeeper 1*, which is now ready. The HiPath AP 1140 is registered with *HiPath gatekeeper 1*.

HiPath Gatekeeper Unreachable

There are two HiPath gatekeepers, *HiPath gatekeeper 1* and 2. There are two HiPath AP 1140s, the HiPath AP 1140 #1 and the HiPath AP 1140 #2.

The two HiPath gatekeepers are configured to accept the registration requests from the two HiPath AP 1140s. The value of the *Retry time* field is set to 1 minute for both HiPath AP 1140s.

1. The HiPath AP 1140 #1 is registered to *HiPath gatekeeper 1*.
2. The HiPath AP 1140 #2 is registered to *HiPath gatekeeper 1*.
3. *HiPath gatekeeper 1* has a hard disk failure and becomes non-operational.
4. Eventually, the user of the HiPath AP 1140 #1 picks up the handset and dials the extension of the HiPath AP 1140 #2.
5. The HiPath AP 1140 sends the admission request message to *HiPath gatekeeper 1*, which is not operational. The admission request times out. The HiPath AP 1140 #1 now considers itself unregistered since *HiPath gatekeeper 1* is not responding.
6. The call between the HiPath AP 1140 #1 and the HiPath AP 1140 #2 fails. The user of the HiPath AP 1140 #1 hangs-up.
7. The HiPath AP 1140 waits one (1) minute before trying to register.
8. The HiPath AP 1140 tries to register to *HiPath gatekeeper 1* but the registration request times out. *HiPath gatekeeper 1* is non-operational.
9. The HiPath AP 1140 tries to register to *HiPath gatekeeper 2*, which is ready. The HiPath AP 1140 is registered to *HiPath gatekeeper 2*.

Steps 4 to 9 also apply for the HiPath HiPath AP 1140 #2.

Ports Configuration

This chapter defines how to configure each FXS port of the HiPath AP 1140. This includes setting functional parameters such as location, sound levels, etc. It also allows to define how each FXS port handles incoming and outgoing calls.

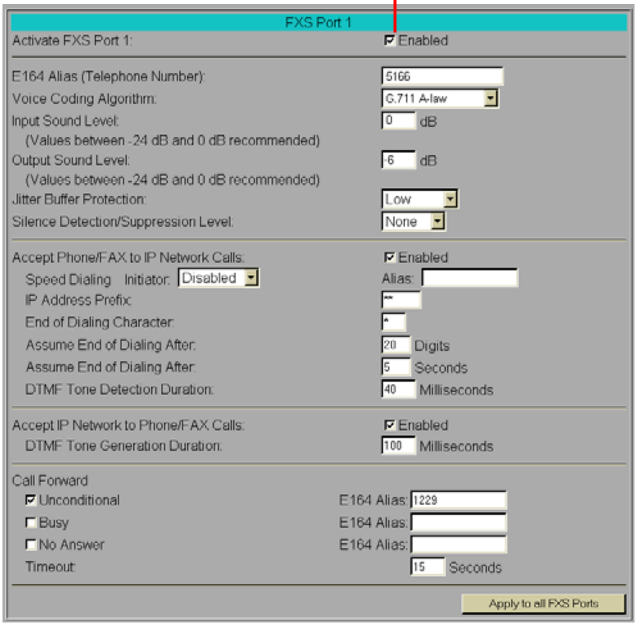
Configuring Incoming and Outgoing Calls Parameters

Each FXS section has a master switch (the *Enabled* check box) to enable or disable a specific port. When a port is disabled, it cannot make nor receive calls.

> When a telephone connected to one of the FXS ports is put on-hook, the HiPath AP 1140 signals this by performing a current loop drop. The current loop drop, also referred to Power Denial mode by some manufacturers, is typically used for disconnect supervision. It signals that the remote telephone has been taken on-hook. The HiPath AP 1140 will detect a Current Drop if this signal is maintained for at least 600 ms with an open circuit or has a current drop lower than 0.4 mA.

Figure 14: FXS Port 1 Section

Master switch to enable/disable the port



FXS Port 1

Activate FXS Port 1: ☑ Enabled

E164 Alias (Telephone Number): 5166
Voice Coding Algorithm: G.711 A-law
Input Sound Level: 0 dB
(Values between -24 dB and 0 dB recommended)
Output Sound Level: -6 dB
(Values between -24 dB and 0 dB recommended)
Jitter Buffer Protection: Low
Silence Detection/Suppression Level: None

Accept Phone/FAX to IP Network Calls: ☑ Enabled
Speed Dialing Initiator: Disabled Alias:
IP Address Prefix: **
End of Dialing Character: *
Assume End of Dialing After: 20 Digits
Assume End of Dialing After: 5 Seconds
DTMF Tone Detection Duration: 40 Milliseconds

Accept IP Network to Phone/FAX Calls: ☑ Enabled
DTMF Tone Generation Duration: 100 Milliseconds

Call Forward
☑ Unconditional E164 Alias: 1229
☐ Busy E164 Alias:
☐ No Answer E164 Alias:
Timeout 15 Seconds

All parameters can be identical for each FXS port. If this is what you want, click *Apply to All FXS Ports* in the *FXS Port 1* section once the parameters are set.

If you want to assign different values to each FXS port, you can do so by enabling the corresponding *FXS Port* section.

The FXS Port sections contain four (4) settings categories:

- Telephony settings
- Accept Phone/Fax to IP Network call settings
- Accept IP Network to Phone/Fax call settings.
- Call Forward Settings

Telephony Settings

The following table describes the telephony parameters that can be set:

Parameter	**Definition**
E.164 Alias (Telephone Number)	The E.164 alias corresponds to the telephone number of each FXS port of the HiPath AP 1140. This telephone number will be used by outside users who want to call this specific FXS port. The value of this field is used in the registration process. If the selected type of gatekeeper is *HiPath Gatekeeper*, the value of this field must be the same as the extension of the HiPath gatekeeper subscriber associated with the FXS port. The telephone number assigned to the FXS port must not contain any spaces, dots or '-', for example: 8298749. **Value**: A string of up to 50 characters from “0” to “9”, “*”, and “,”. **Default value**: none (empty field).

Parameter	Definition
Voice Coding Algorithm	The preferred voice-coding algorithm used by the FXS port when placing calls. See “Selecting the Proper Codec” on page 48 for more details. **Value**: G.711 A-law, G.711 µ-law, G.723, FAX, T.38 FAX, T.38 FAX ONLY **Default Value**: G.711 A-law. **Notes**: – Fax transmission is supported in Voice Band Data (VBD) over the G.711 codec with any setting, except *T.38 FAX ONLY* and *G.723.* The G.723 voice-coding algorithm cannot be used for fax transmissions. – When selecting *T.38 FAX*, if both units are T.38 capable, T.38 will be used for fax; otherwise, transmission in clear channel over G.711 will be used. – When selecting *T.38 FAX ONLY*, if both units are T.38 capable, T.38 will be used for fax; otherwise, the call will be rejected.
Input Sound Level	The sound level, in dB, received by the HiPath AP 1140. Values range from +12 dB to -36 dB by increments of 1. Note that values below -24 dB or above 0 dB are not recommended. **Default Value**: 0 dB
Output Sound Level	The sound level, in dB, received by the HiPath AP 1140. Values range from +12 dB to -36 dB by increments of 1. Note that values below -24 dB or above 0 dB are not recommended. **Default Value**: -6 dB

Parameter	Definition
Jitter Buffer Protection	The level of jitter buffer protection, which provides better protection against packet loss, but increases the voice delay. If the network to which the HiPath AP 1140 is connected suffers from a high level of congestion, the level of jitter buffer protection should be higher. If the network to which the HiPath AP 1140 is connected suffers from a low level of congestion, the level of jitter buffer protection should be lower. **Value**: Very low, Low, High, Very high **Default Value**: Low
Silence Detection/ Suppression Level	The level of silence detection/suppression. A high level can chop some part of the voice transfers. **Values**: None, Low (transparent), Normal (conservative), High (aggressive) **Note**: The difference between transparent and conservative is how "aggressive" the algorithm will consider something as an inactive voice and how "fast" it will stop the voice stream. A setting of conservative is a little bit more aggressive to react to silence compared to a setting of transparent. **Default**: None

Selecting the Proper Codec

The following table will help you understand which codecs are available according to the codec you have selected.

Selected codec	Preferred codec when negociating with remote unit	Available codecs in voice mode	Available codecs when switching to Fax mode
G.711 A-Law	G.711 A-Law	G.711µ-law, G.711 A-Law, G.723.1	G.711µ-law
G.711µ-law	G.711µ-law	G.711µ-law, G.711 A-Law, G.723.1	G.711µ-law
G.723.1	G.723.1	G.711µ-law, G.711 A-Law, G.723.1	G.711µ-law

Selected codec	Preferred codec when negociating with remote unit	Available codecs in voice mode	Available codecs when switching to Fax mode
FAX	G.711µ-law	G.711µ-law, G.711 A-Law	G.711µ-law
T.38 FAX	G.711µ-law	G.711µ-law, G.711 A-Law	T.38 over TCP, G.711µ-law
T.38 FAX ONLY	Accepts G.711µ-law at initialization, but the transmission is cut immediately	N/A	T.38 over TCP

Accept Phone/Fax to IP Network Call Settings

An analog device connected to the HiPath AP 1140 can place a call on the IP network to which the HiPath AP 1140 is connected. The following table describes the parameters that can be set:

Parameter	Definition
Accept Phone/Fax to IP Network call	When the *Enabled* option is checked, the FXS port can make outgoing calls to the IP network.
Speed Dialing – Initiator	Permits fast dialing of a pre-defined number defined in the *Alias* field on the right. **Value**: Disabled, Automatic, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, *, # When *Automatic* is selected, the *Alias* is automatically dialed when the handset is taken off hook. In this case, the following features are not used: *End of dialing character*, *Assume end of dialing after*, *DTMF tone duration*. When using values other than *Disabled* and *Automatic*, the *Alias* is dialed when the selected value is pressed on the phone keypad (e.g. 9). This value must be the first digit entered. For instance, dialing *9* will start the speed dialing, while dialing *192* will not. **Note**: The *Speed Dialing Initiator* must be different from the *End of Dialing Character.* **Default Value**: Disabled

Parameter	Definition
Speed Dialing – Alias	Number to call. This number can be: – A phone number/E.164 alias (e.g.: 10048) – An IP address (e.g.: 15.2.3.45) – An IP address with a phone number (e.g.: 15.2.3.45:10048). This is used if you want to call a specific phone on a 4-ports HiPath AP 1140 terminal. This alias will be called automatically when the handset is off hook if the *Initiator* is *Automatic*, or it will be called when the selected *Initiator* value is pressed on the phone keypad. **Note**: If the HiPath AP 1140 is registered to a gatekeeper and you use an IP address in the Speed Dial, the call is not processed. You will get a dialtone and will be able to normally make a call.
IP Address Prefix	Prefix used when dialing an IP address. For example, the IP address prefix could be **. To call a terminal with IP address 192.168.0.1, you would thus dial as follows: **192*168*0*1* **Notes**: – When the IP address prefix is recognized, the rule for the automatic speed dial is not checked anymore. – Calls using an IP address are not possible when the HiPath AP 1140 is configured to register with a gatekeeper. **Default Value**: **

Parameter	Definition
End of Dialing Character	Character that indicates the end of the dialing sequence. It will not be part of the dialing sequence. If this field is left empty, it is assumed you are not using this option. **Notes**: – This rule applies only to telephone numbers (E.164 aliases). It does not apply to IP addresses. – This option is not used if the *Initiator* value is *Automatic*. – The *Speed Dialing Initiator* must be different from the *End of Dialing Character*. **Value**: *, #, empty field **Default Value**: *
Assume End of Dialing After *n* digits	Number of digits after which the call is processed. Make sure that this number properly matches the number of digits in the call number. **Notes**: – This rule applies only to telephone numbers (E.164 aliases). It does not apply to IP addresses. – This option is not used if the *Initiator* value is *Automatic*. **Value**: Any number between 1 and 20 **Default Value**: 20

Parameter	Definition
Assume End of Dialing after *n* seconds	Time, in seconds, to wait after the last digit is dialed before processing the call. **Notes**: – This rule applies to telephone numbers (E.164 aliases) and IP addresses. – This option is not used if the *Initiator* value is *Automatic*. **Default Value**: 5 seconds
DTMF Tone Detection Duration	Time length defined to detect incoming DTMFs. Shorter the detection duration, higher are error risks. Longer the detection duration, higher are the risks of missing a DTMF. **Value**: Any number of milliseconds between 40 and 150. **Default Value**: 40 ms

IP Network to Phone/Fax Call Settings

An analog device connected to the HiPath AP 1140 can receive a call from the IP network to which the HiPath AP 1140 is connected. The following table describes the parameters that can be set:

Parameter	Definition
Accept IP Network to Phone/Fax call	When the *Enabled* option is checked, the FXS port can receive calls from the IP Network.
DTMF Tone Generation Duration	The time length DTMFs are played when making a call. **Value**: Any number of milliseconds between 40 and 150. **Default Value**: 100 ms

Call Forward Settings

The HiPath AP 1140 can use three types of call forwards:

- Unconditional
- Busy
- No Answer

The *Busy* and *No Answer* options can be selected at the same time, but you cannot select any of them if you have checked the *Unconditional* option.

The Call Forward settings are automatically effective and will not require the HiPath AP 1140 to reboot.

The following table describes the parameters that can be set.

Parameter	**Definition**
Unconditional	Forwards calls to another endpoint. Enter its E.164 alias in the field on the right.
Busy	Automatically forwards incoming calls to a pre-determined endpoint if you are already on the line. Enter its E.164 alias in the field on the right.
No Answer	Automatically forwards incoming calls to a pre-determined endpoint if you do not answer before a specific number of seconds, which is defined in the *Timeout* field. Enter its E.164 alias in the field on the right.
Time out	In the Call forward – No Answer scenario, number of seconds after which the call is forwarded to the defined endpoint. The default value is 15 seconds.

Setting the Call Forward Destination

When selecting one of the call forward options, you must set the destination of the call related to this option.

Parameter	**Definition**
Type	Type of destination. – **E.164 Alias**: Telephone number attributed to an endpoint. This endpoint can be anything that supports E.164 aliases such as the ports of terminals, IP phones, etc.

Miscellaneous Configuration

This chapter describes other configuration settings not covered in the previous chapters.

Quality of Service Settings

QoS (Quality of Service) features enable network managers to decide on packet priority queuing. QoS is the ability of a network element (e.g. an application, host or router) to have some level of assurance that its traffic and service requirements can be satisfied.

There are a number of characteristics that qualify QoS, including:

- minimizing delivery delay
- minimizing delay variations
- providing consistent data throughput capacity

What are Differentiated Services?

Differentiated Services (DiffServ, or DS) is a protocol for specifying and controlling network traffic by class so that certain types of traffic get precedence – for example, voice traffic, which requires a relatively uninterrupted flow of data, might get precedence over other kinds of traffic.

Differentiated Services avoids simple priority tagging and depends on more complex policy or rule statements to determine how to forward a given network packet. An analogy is made to travel services, in which a person can choose among different modes of travel – train, bus, airplane – degree of comfort, the number of stops on the route, standby status, the time of day or period of year for the trip, and so forth.

For a given set of packet travel rules, a packet is given one of 64 possible forwarding behaviors – known as per hop behaviors (PHBs). A six-bit field, known as the Differentiated Services Code Point (DSCP), in the Internet Protocol (Internet Protocol) header specifies the per hop behavior for a given flow of packets. The DS field structure is presented below:

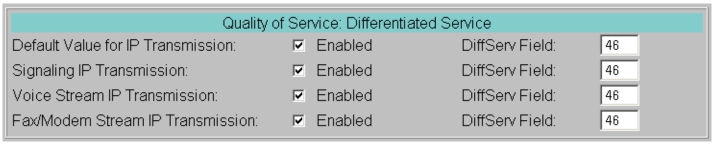
```
0   1   2   3   4   5   6   7
+---+---+---+---+---+---+---+---+
| DSCP                  |  CU   |
+---+---+---+---+---+---+---+---+
```

- *DSCP*: Differentiated Services CodePoint.
- *CU*: Currently Unused. The CU bits should always be set to 0.

Differentiated Services (DiffServ) Section

You can set various Differentiated Services parameters that will allow you to control the network traffic.

Figure 15: Differentiated Service Configuration Section



Quality of Service: Differentiated Service

Default Value for IP Transmission: ☑ Enabled DiffServ Field: 46

Signaling IP Transmission: ☑ Enabled DiffServ Field: 46

Voice Stream IP Transmission: ☑ Enabled DiffServ Field: 46

Fax/Modem Stream IP Transmission: ☑ Enabled DiffServ Field: 46

The following table describes the parameters that can be set:

Parameter	Definition
Default Value for IP Transmission	One (1) octet scalar that defines the default IP transmission. You must check the *Enabled* option to use the DiffServ value. **Value**: Any number between 0 and 63. **Note**: If the HiPath AP 1140 is set to register with a HiPath Gatekeeper, the autodiscovery feature of the HiPath 5000 system will overwrite any value entered in this field. See "Setting up Gatekeeper Information" on page 33 for more details. **Default Value**: 46
Signaling IP Transmission	One (1) octet scalar that defines a signalling filter on your router to take advantage of priority queuing. You must check the *Enabled* option to use the DiffServ value. **Value**: Any number between 0 and 63. **Note**: If the HiPath AP 1140 is set to register with a HiPath Gatekeeper, the autodiscovery feature of the HiPath 5000 system will overwrite any value entered in this field. See "Setting up Gatekeeper Information" on page 33 for more details. **Default Value**: 46

Parameter	Definition
Voice Stream IP transmission	One (1) octet scalar that defines a media filter on your router to take advantage of voice transmission priority queuing. You must check the *Enabled* option to use the DiffServ value. **Value**: Any number between 0 and 63. **Note**: If the HiPath AP 1140 is set to register with a HiPath Gatekeeper, the autodiscovery feature of the HiPath 5000 system will overwrite any value entered in this field. See "Setting up Gatekeeper Information" on page 33 for more details. **Default Value**: 46
Fax/Modem Stream IP transmission	One (1) octet scalar that defines a media filter on your router to take advantage of fax/modem transmission priority queuing. You must check the *Enabled* option to use the DiffServ value. **Value**: Any number between 0 and 63. **Note**: If the HiPath AP 1140 is set to register with a HiPath Gatekeeper, the autodiscovery feature of the HiPath 5000 system will overwrite any value entered in this field. See "Setting up Gatekeeper Information" on page 33 for more details. **Default Value**: 46

The proposed default values of 46 (or binary 101110) are based on the Expedited Forwarding PHB (RFC 2598) recommendation. This default value would also result in "101" precedence bits, low delay, high throughput, and normal reliability in the legacy IP networks (RFC 791, RFC 1812). Network managers of legacy IP networks could use the above-mentioned values to define filters on their routers to take advantage of priority queuing.

You can find references on the DS field under the IETF working group DiffServ. For more information, please refer to the following RFC documents:

- Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers (RFC 2474)
- An Architecture for Differentiated Services (RFC 2475)
- Assured Forwarding PHB Group (RFC 2597)

- An Expedited Forwarding PHB (RFC 2598)

802.1q Section

The 802.1q standard recommends the use of the 802.1q VLAN tags for Ethernet frames traffic prioritization. VLAN tags are 4-byte headers in which three bits are reserved for priority indication.

> If you enable 802.1q and set a VLAN ID for the HiPath AP 1140, the Web pages, TFTP and Syslog **must** be on a computer (Network Card) set with the same VLAN ID.

For both signaling and media packets, the VLAN priority section is configurable independently.

VLANs

VLANs are created with standard Layer 2 Ethernet. A VLAN Identifier (VID) is associated with each VLAN. VLANs aim to offer the following benefits:

- VLANs are supported over all IEEE 802 LAN MAC protocols, and over shared media LANs as well as point-to-point LANs.
- VLANs facilitate easy administration of logical groups of stations that can communicate as if they were on the same LAN. They also facilitate easier administration of moves, adds, and changes in members of these groups.
- Traffic between VLANs is restricted. Bridges forward unicast, multicast, and broadcast traffic only on LAN segments that serve the VLAN to which the traffic belongs.
- As far as possible, VLANs maintain compatibility with existing bridges and end stations.

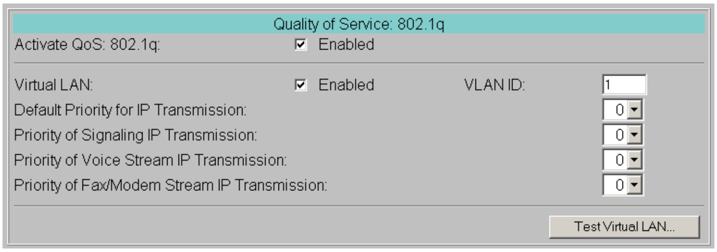
The VLAN field in the Ethernet file is located after both destination and source addresses:

```
0                   1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7   (byte)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
| Dest Addr | Src Addr  | VLAN  | Type/Length | ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

The VLAN field is separated as follows:

```
0  (bit)            1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             0x8100            | Pri |T|          VID          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 16: 802.1q Configuration Section



Quality of Service: 802.1q

Activate QoS: 802.1q: ☑ Enabled

Virtual LAN: ☑ Enabled VLAN ID: 1

Default Priority for IP Transmission: 0

Priority of Signaling IP Transmission: 0

Priority of Voice Stream IP Transmission: 0

Priority of Fax/Modem Stream IP Transmission: 0

The following table describes the parameters that can be set:

Parameter	Definition
Activate QoS: 802.1q	Enables the 802.1q settings.
Virtual LAN	Virtual LAN located in the VLAN field. You must check the *Enabled* option to use the Virtual LAN value. **Value**: Any number between 1 and 4096. **Default Value**: 1
Default Priority for IP Transmission	Default priority value for IP transmissions located in the VLAN field. **Value**: Any number between 0 and 7. **Default Value**: 0
Priority of Signaling IP Transmission	Priority value for signalling IP transmissions located in the VLAN field. **Value**: Any number between 0 and 7. **Default Value**: 0

Parameter	Definition
Priority of Voice Stream IP Transmission	Priority value for voice stream IP transmission located in the VLAN field. **Value**: Any number between 0 and 7. **Default Value**: 0
Priority of Fax/ Modem Stream IP Transmission	Priority value for fax/modem stream IP transmission located in the VLAN field. **Value**: Any number between 0 and 7. **Default Value**: 0

Testing the Virtual LAN

If you enable the 802.1q service, it could have a major impact on the network and not necessarily all devices connected to this network are able to accommodate it.

To verify if your network and the devices that are connected to it support the 802.1q service, the HiPath AP 1140 offers the option to place the unit in 802.1q mode for a few minutes. This is done by clicking the *Test Virtual LAN* button.

In the minutes following the activation of this service, Siemens AG recommends to proceed with actions to validate the communication with your HiPath AP 1140 units.

Note on the Implementation of the IEEE Standard 802.1q

This note applies only for previous hardware revisions that do not use revision D of the main CPU, the Motorola PowerPC 860.

The implementation of the IEEE Standard 802.1q in the HiPath AP 1140 has a minor problem due to hardware limitations. 802.1q increases the Ethernet frame header by 4 bytes, adding a Virtual LAN ID and a user_priority. This is useful to limit broadcasts that cross bridges, and it may also prioritize frames in the queuing algorithm of switches. However, it also increases the maximum possible size of Ethernet frames from 1518 to 1522 bytes, and this might not be handled adequately by every hardware.

PCs running Windows can use a workaround to avoid sending 1522 bytes packets (note that this happens only in special and rare cases). The workaround is to reduce the MTU of the interface (the one that sends packets with 802.1q framing) by 4 bytes.

- Use the registry editor (regedt32 on Windows 2000) and go to the key:

  ```
  \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<ethernet
  adapter>\Parameters\Tcpip
  ```

  `where <Ethernet adapter> can be found by using the command “ipconfig / all”.`

- Add (or modify) a value named MTU of type REG_DWORD. Set it to 1496 (instead of 1500), in decimal. Reboot the computer to have those changes in effect.
- To validate that your changes are correct, try to ping the HiPath AP 1140 with large packets once rebooted:

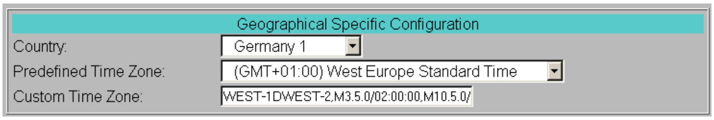
  ```
  ping -l 2000
  ```

This will cause IP fragmentation, the first fragment being as large as the interface allows it. With the MTU reduced, you should now receive an answer. You can even ping with packets of 65500 bytes!

Geographical Specific Configuration

This section allows you to define the country and time zone in which the HiPath AP 1140 is located.

Figure 17: Geographical Specific Configuration Window



Geographical Specific Configuration

Country: Germany 1

Predefined Time Zone: (GMT+01:00) West Europe Standard Time

Custom Time Zone: WEST-1DWEST-2,M3.5.0/02:00:00,M10.5.0/

The following parameters can be set:

Parameter	Description
Country	The country in which the HiPath AP 1140 is located. Selecting a country automatically sets the parameters specific to this country. See “Appendix B – Country Specific Parameters” on page 101 for parameters specific to each supported country. **Value**: Europe, Austria, France, Germany 1, Germany 2, Great Britain, Italy, North America 1, North America 2, Spain, Switzerland **Default Value**: Germany 1
Predefined Time Zone	List of pre-defined time zones. See “Selecting a Time Zone” on page 62 for more details.
Custom Time Zone	String of the selected time zone. If you have selected custom time zone, enter your own time zone string as explained in “Defining a Custom Time Zone” on page 64.

Selecting a Time Zone

At boot time, the HiPath AP 1140 queries a SNTP or NTP server to receive time information (see “SNTP Settings” on page 66 for more details). The unit receives the information in Greenwich Mean Time (GMT) format, so it needs to convert this GMT time into the proper time zone. To do this, the HiPath AP 1140 offers time zone configuration with daylight saving settings. The clock is automatically adjusted for daylight saving time changes, if applicable. Available values are:

- – (GMT-08:00) Pacific Time (Canada & US)

- (GMT-07:00) Mountain Time (Canada & US)
- (GMT-06:00) Central Time (Canada & US)
- (GMT-05:00) Eastern Time (Canada & US)
- (GMT-04:00) Atlantic Time (Canada&US)
- (GMT) Greenwich Mean Time
- (GMT+01:00) West Europe Standard Time
- (GMT+08:00) China Standard Time
- (GMT+09:00) Tokyo Standard Time
- (GMT+09:30) Central Australia Standard Time
- (GMT+10:00) Australia Eastern Standard Time

The default value is **Pacific Time (Canada & US) (GMT - 8h)**. The pre-configured time zones available are:

Time zone	**GMT Offset**	**Daylight saving time**			**POSIX String**
		GMT Offset	**Starting Date**	**Ending Date**	
Pacific Time (Canada & US)	-08:00	-07:00	1st Sunday of April at 02:00:00 AM	Last Sunday of October at 02:00:00 AM	PST8DST7,M4.1.0/02:00:00,M10.5.0/02:00:00
Mountain Time (Canada & US)	-07:00	-06:00	1st Sunday of April at 02:00:00 AM	Last Sunday of October at 02:00:00 AM	MST7DST6,M4.1.0/02:00:00,M10.5.0/02:00:00
Central Time (Canada & US)	-06:00	-05:00	1st Sunday of April at 02:00:00 AM	Last Sunday of October at 02:00:00 AM	CST6DST5,M4.1.0/02:00:00,M10.5.0/02:00:00
Eastern Time (Canada & US)	-05:00	-04:00	1st Sunday of April at 02:00:00 AM	Last Sunday of October at 02:00:00 AM	EST5DST4,M4.1.0/02:00:00,M10.5.0/02:00:00
Atlantic Time (Canada)	-04:00	-03:00	1st Sunday of April at 02:00:00 AM	Last Sunday of October at 02:00:00 AM	AST4DST3,M4.1.0/02:00:00,M10.5.0/02:00:00
GMT Standard Time	-00:00	+01:00	Last Sunday of March at 01:00:00 AM	Last Sunday of October at 02:00:00 AM	GMT0DMT-1,M3.5.0/01:00:00,M10.5.0/02:00:00
W. Europe Standard Time	+01:00	+02:00	Last Sunday of March at 02:00:00 AM	Last Sunday of October at 03:00:00 AM	WEST-1DWEST-2,M3.5.0/01:00:00,M10.5.0/03:00:00
China Standard Time	+08:00	None	N/A	N/A	CST-8
Tokyo Standard Time	+09:00	None	N/A	N/A	TST-9

Time zone	GMT Offset	Daylight saving time			POSIX String
		GMT Offset	Starting Date	Ending Date	
Central Australia Standard Time	+09:30	+10:30	Last Sunday of October at 02:00:00 AM	Last Sunday of March at 02:00:00 AM	CAUST-9:30DCAUST-10:30,M10.5.0/02:00:00,M3.5.0/02:00:00
Australia Eastern Standard Time	+10:00	+11:00	Last Sunday of October at 02:00:00 AM	Last Sunday of March at 02:00:00 AM	AUSEST-10AUSDST-11,M10.5.0/02:00:00,M3.5.0/02:00:00

Defining a Custom Time Zone

To define a custom time zone, you must enter a valid POSIX (Portable Operating System Interface) string in the *Custom Time Zone* field. A POSIX string is a set of standard operating system interfaces based on the UNIX operating system. This standard is used in the time zone string in the format:

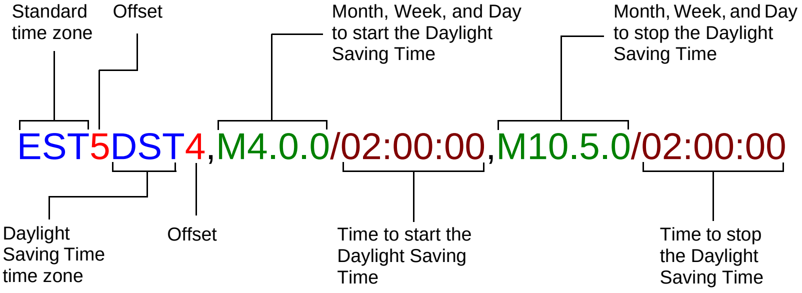
```
STD[OFFSET]DLST[OFFSET],[START[/TIME]],[END[/
TIME]]
```

Setting	Definition
STD DLST	Three or more characters for the standard (STD) or alternative daylight saving time (DLST) time zone. Only STD is mandatory. If DLST is not supplied, the daylight saving time does not apply. Lower and upper case letters are allowed. All characters are allowed except digits, leading colon (:), comma (,), minus (-), plus (+), and ASCII NUL.
OFFSET	Difference between the local time and the GMT time. The offset has the format *h[h][:m[m][:s[s]]]*. If no offset is supplied for DLST, the alternative time is assumed to be one hour ahead of standard time. One or more digits can be used; the value is always interpreted as a decimal number. The hour value must be between 0 and 24. The minutes and seconds values, if present, must be between 0 and 59. If preceded by a minus (-), the time zone is east of the prime meridian, otherwise it is west, which can be indicated by the preceding plus sign (+). For example, New York time is GMT+5.

Setting	Definition
START END	Indicates when to change to and return from the daylight saving time. The *START* argument is the date when the change from the standard to the daylight save time occurs; *END* is the date for changing back. If *START* and *END* are not specified, the default is the US Daylight saving time start and end dates. The format for start and end must be **one** of the following: – **n** where *n* is the number of days since the start of the year from 1 to 365. It must contain the leap year day if the current year is a leap year. With this format, it is your responsibility to determine all the leap year details. – **Jn** where *n* is the number of days since the start of the year from 1 to 365. Leap days are not counted. The *TIME* parameter has the same format as *OFFSET* but there can be no leading minus (-) or plus (+) sign. If *TIME* is not specified, the default is *02:00:00*. – **Mx[x].y.z** where *x* is the month, *y* is a week count and *z* is the day of the week starting at 0 (Sunday). As an example, *M10.5.0* is the Sunday of the fifth week of October. The *TIME* parameter has the same format as *OFFSET* but there can be no leading minus (-) or plus (+) sign. If TIME is not specified, the default is *02:00:00*.

Example

The following is an example of a proper POSIX string:

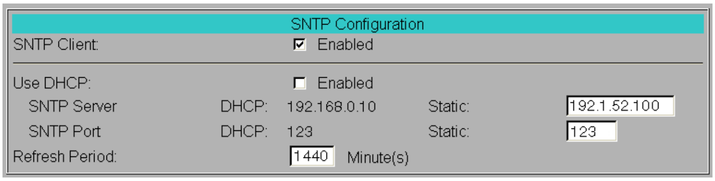

Standard time zone
Offset
Month, Week, and Day to start the Daylight Saving Time
Month, Week, and Day to stop the Daylight Saving Time
EST5DST4,M4.0.0/02:00:00,M10.5.0/02:00:00
Daylight Saving Time time zone
Offset
Time to start the Daylight Saving Time
Time to stop the Daylight Saving Time

SNTP Settings

The Simple Network Time Protocol (SNTP) enables the notion of time (date, month, time) into the HiPath AP 1140. It is especially required when dealing with features such as the Caller ID.

SNTP is used to synchronize a SNTP client with a SNTP or NTP server (SNTP being a subset of NTP) by using UDP as transport (see RFC 1769 for more details).

Figure 18: SNTP Configuration Window



SNTP Configuration

SNTP Client: ☑ Enabled

Use DHCP: ☐ Enabled

SNTP Server DHCP: 192.168.0.10 Static: 192.1.52.100

SNTP Port DHCP: 123 Static: 123

Refresh Period: 1440 Minute(s)

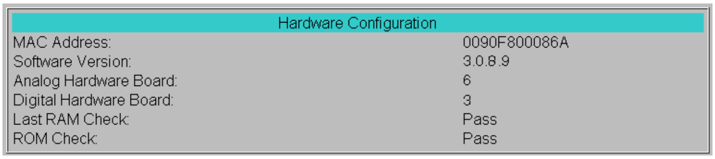
The following settings can be defined.

Variable	Description
SNTP Client	Check the *Enabled* option to enable the SNTP feature in the HiPath AP 1140.
Use DHCP	When the *Enabled* option is checked, the HiPath AP 1140 receives the SNTP server IP address and Port number via a DHCP server. If you want to enter a static IP address and port number, uncheck the *Enabled* option and enter the information in the *SNTP Server* and *SNTP Port* static fields.
Refresh Period	Interval, in minutes, before sending a SNTP time request to the SNTP server. Available values are between 1 and 1440 minutes. **Default Value**: 1140

Viewing Hardware Information

This read-only section lists the hardware configuration information.

Figure 19: Hardware Configuration Section



Hardware Configuration

MAC Address:	0090F800086A
Software Version:	3.0.8.9
Analog Hardware Board:	6
Digital Hardware Board:	3
Last RAM Check:	Pass
ROM Check:	Pass

The following table describes the parameters that can be viewed:

Parameter	Definition
MAC Address	MAC address of the HiPath AP 1140.
Software Version	Software version of the HiPath AP 1140.
Analog Hardware Board	Version of the analog circuit board of the HiPath AP 1140.
Digital Hardware Board	Version of the digital circuit board of the HiPath AP 1140.
Last RAM Check	Lets you know if the RAM on the HiPath AP 1140 is corrupted. If you want to perform a RAM check, click the *RAM Check* button. See “Performing a RAM Check” on page 67 for more details.
ROM Check	Lets you know if the ROM on the HiPath AP 1140 is corrupted. A ROM check is executed each time the HiPath AP 1140 is restarted. If you want to perform a ROM check, click the *ROM Check* button. See “Performing a ROM Check” on page 68 for more details.

Performing a RAM Check

Clicking the *RAM Check* button restarts the HiPath AP 1140 to perform the RAM check. If the HiPath AP 1140 is in use when you click *RAM Check*, it is not restarted and the RAM check is not processed. A warning message informs you of this situation.

If the HiPath AP 1140 is not in use when you click *RAM Check*, a message informs you that the unit is about to restart to perform a RAM check. Approximately 10-20 seconds after receiving this message, you can request the HiPath AP 1140 web pages again to see the result of the RAM check (displayed on the *Overview* and *Configuration* web pages).

Performing a ROM Check

Clicking the *ROM Check* button starts a ROM check. If the HiPath AP 1140 is in use when you click *ROM Check*, the ROM check is not processed. A warning message informs you of this situation.

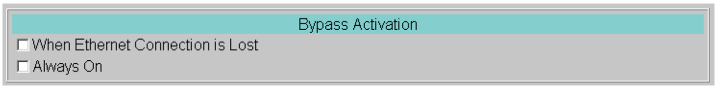
If the HiPath AP 1140 is not in use when you click *ROM Check*, a ROM check is performed. A message informs you of the result.

System Failure Bypass Activation Section

The HiPath AP 1140 has a fifth RJ-11 connector used to connect to a standard SCN line, called *Bypass.*

In the event of a commercial power failure or network failure, this feature permits users to make and receive calls even when the HiPath AP 1140 is not operating.

Figure 20: Bypass Activation Section



Bypass Activation

☐ When Ethernet Connection is Lost

☐ Always On

During normal operation, the SCN line connected to the *Bypass* port is switched out of the circuit through commuting relays. When power is removed from the HiPath AP 1140, or if the IP network is in down conditions, the relay is mechanically restored to a connected state and the SCN line can be used as an emergency line. Consequently, a phone/fax used on FXS Port 1 will be directly connected to this SCN line.

When the error conditions have been cleared or the power is restored, Port 1 stays in System Failure Bypass connection until the device connected to it is on-hook. This safety feature ensures that an emergency call does not get disconnected from the SCN.

Setting the Bypass Activation

The following table describes the parameters that can be set:

Parameter	Definition
When Ethernet connection is lost	The System Failure Bypass is activated if the Ethernet connection is lost. **Note**: The System Failure Bypass is always activated in case of power loss.
Always on	The System Failure Bypass is activated in the following cases: – Power is removed from the HiPath AP 1140. – Power is recovered but a System Failure Bypass call is still in progress. – Network is down. – Network connection is recovered but a System Failure Bypass call is still in progress. – The HiPath AP 1140 is in maintenance or test mode.

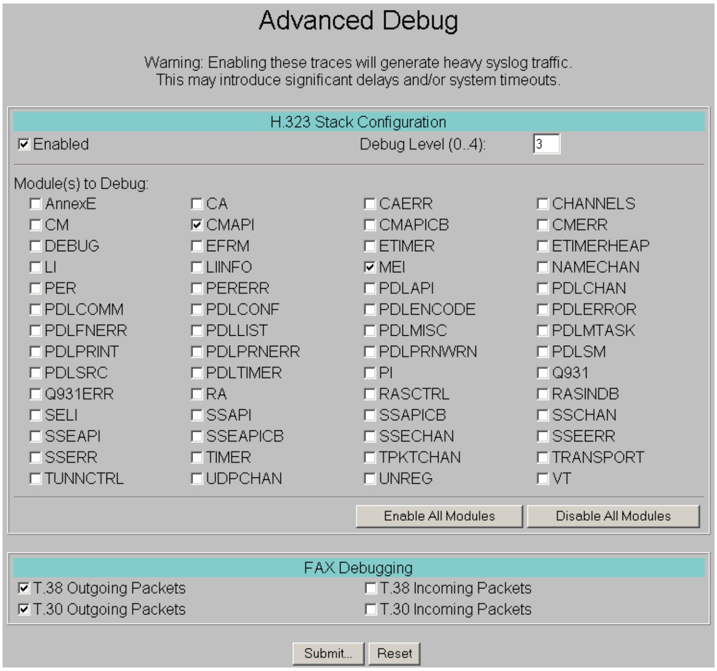
Advanced Debugging

The advanced debug page produces output for debugging, monitoring and tracking the HiPath AP 1140 application. The advanced debug page provides:

- A full picture of all H.323 events on the network, from the perspective of the instance that is generating the log.
- Details about the fields in the messages.
- A decoded view of each message, including the message fields and the value of each field.
- An encoded view as a hexadecimal dump, useful for automatic processing such as automatic debugging tools.

> Enabling the debug traces will generate heavy syslog traffic. This may introduce significant delays and/or system timeouts.

Figure 21: Advanced Debug Page



Advanced Debug

Warning: Enabling these traces will generate heavy syslog traffic.
This may introduce significant delays and/or system timeouts.

H.323 Stack Configuration

☑ Enabled

Debug Level (0..4): 3

Module(s) to Debug:

☐ AnnexE	☐ CA	☐ CAERR	☐ CHANNELS
☐ CM	☑ CMAPI	☐ CMAPICB	☐ CMERR
☐ DEBUG	☐ EFRM	☐ ETIMER	☐ ETIMERHEAP
☐ LI	☐ LIINFO	☑ MEI	☐ NAMECHAN
☐ PER	☐ PERERR	☐ PDLAPI	☐ PDLCHAN
☐ PDLCOMM	☐ PDLCONF	☐ PDLENCODE	☐ PDLERROR
☐ PDLFNERR	☐ PDLLIST	☐ PDLMISC	☐ PDLMTASK
☐ PDLPRINT	☐ PDLPRNERR	☐ PDLPRNWRN	☐ PDLSM
☐ PDLSRC	☐ PDLTIMER	☐ PI	☐ Q931
☐ Q931ERR	☐ RA	☐ RASCTRL	☐ RASINDB
☐ SELI	☐ SSAPI	☐ SSAPICB	☐ SSCHAN
☐ SSEAPI	☐ SSEAPICB	☐ SSECHAN	☐ SSEERR
☐ SSERR	☐ TIMER	☐ TPKTCHAN	☐ TRANSPORT
☐ TUNNCTRL	☐ UDPCHAN	☐ UNREG	☐ VT

FAX Debugging

☑ T.38 Outgoing Packets
☐ T.38 Incoming Packets
☑ T.30 Outgoing Packets
☐ T.30 Incoming Packets

Usage and Benefits

The advanced debug page provides detailed information important for application development and ongoing system maintenance.

Suggestion	Description
Problem Tracking	Provides a chronological record of call events to track exactly where and when a problem occurred.
Interoperability Tracking	Provides an important vehicle for tracking interoperability. You can see if the events on the remote side are interoperable with the events on the local side.

The advanced debug page produces Syslog messages you can see with a Syslog daemon.

Settings

To use the debug options, you must check the *Enabled* check box at the upper left of the window, select the modules you want to debug, then click *Submit*. If you select modules and the *Enabled* check box is not checked, no traces will be produced.

You can customize the output by defining the Debug level.

Level	Meaning
0	Do not display and/or print debug messages. This is the default level.
1	Do not display trees and do not check trees for ASN.1 consistency.
2	Display everything including trees but do not check trees for ASN.1 consistency.
3	Display everything and check trees for ASN.1 consistency, and display inconsistencies found. This is the recommended setting.
4	Display all messages. Note that this setting is not recommended because it generates a lot of traffic.

How to Use the HiPath AP 1140

This chapter describes how to make a phone call or send a fax with the HiPath AP 1140.

HiPath AP 1140 Call Processes

The following examples illustrate some of the various calling processes the HiPath AP 1140 supports. These processes can be adapted at will to suit your needs and requirements.

> When calling a phone or fax on another remote H.323 terminal, you can do so when registered to a gatekeeper or not.

The HiPath AP 1140 can communicate with the following devices:

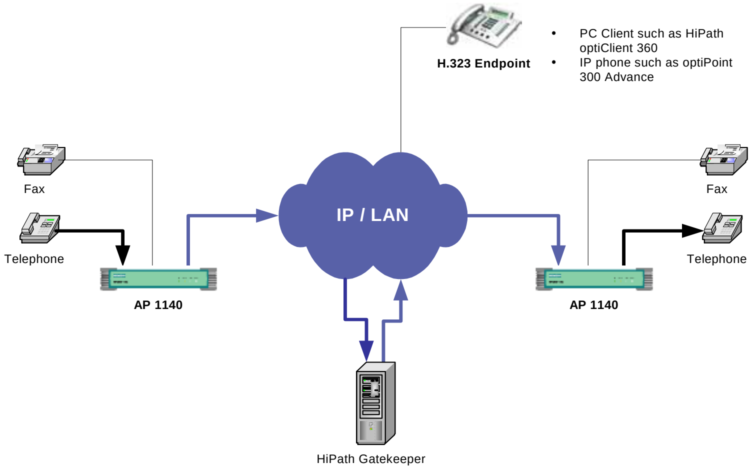
- Another terminal on the IP network such as the HiPath AP 1100 or HiPath AP 1140.
- Any LAN H.323 endpoint on the IP network, for instance:
  - a PC Client such as the HiPath optiClient 360
  - an IP phone such as the optiPoint 300 Advance directly connected to the IP network
- A SCN phone or fax. However, the HiPath AP 1140 would need to contact a SCN gateway such as the HiPath RG 2100 or RG 2500.

Calls Involving Another Terminal

The following example illustrates how to reach a phone or fax on another HiPath AP 1140 terminal.

▶ Phone/Fax -> HiPath AP 1140 A -> HiPath AP 1140 B -> Phone/Fax

A user makes a call with the phone/fax connected to an HiPath AP 1140, which in turn contacts another HiPath AP 1140, then reaches the corresponding phone/fax.


H.323 Endpoint
• PC Client such as HiPath optiClient 360
• IP phone such as optiPoint 300 Advance
Fax
Telephone
AP 1140
IP / LAN
Fax
Telephone
AP 1140
HiPath Gatekeeper

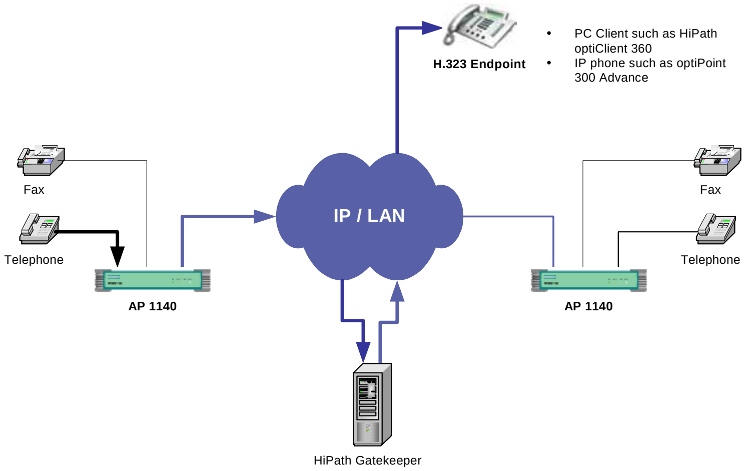
Calls Involving a Terminal and an H.323 Endpoint

The following examples illustrate how a phone/fax connected to an HiPath AP 1140 terminal can communicate with a LAN H.323 endpoint on the IP network. Such endpoints could be:

- a PC Client such as the HiPath optiClient 360
- an IP phone such as the optiPoint 300 Advance directly connected to the IP network

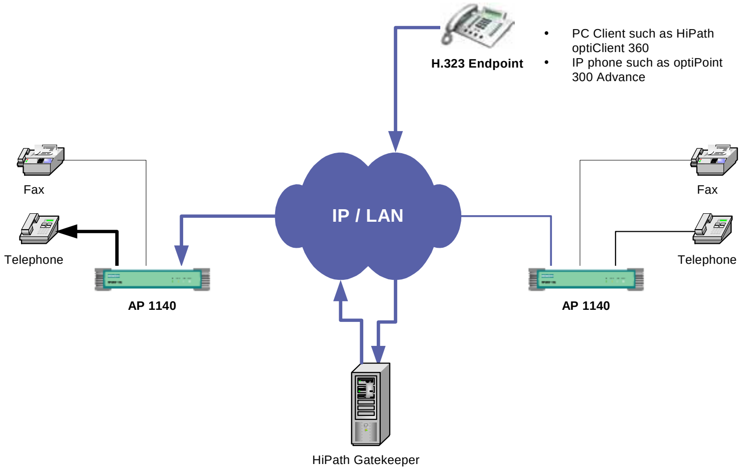
▶ Phone/Fax -> HiPath AP 1140 -> LAN H.323 endpoint

A user makes a call with the phone/fax connected to an HiPath AP 1140, which reaches the corresponding LAN H.323 endpoint on the IP network.


H.323 Endpoint
- PC Client such as HiPath optiClient 360
- IP phone such as optiPoint 300 Advance
Fax
Telephone
AP 1140
IP / LAN
Fax
Telephone
AP 1140
HiPath Gatekeeper

▶ LAN H.323 endpoint -> HiPath AP 1140 -> Phone/Fax

A LAN H.323 endpoint contacts the HiPath AP 1140, which reaches the corresponding phone/fax connected to the HiPath AP 1140 terminal.


H.323 Endpoint
- PC Client such as HiPath optiClient 360
- IP phone such as optiPoint 300 Advance
Fax
Telephone
AP 1140
IP / LAN
Fax
Telephone
AP 1140
HiPath Gatekeeper

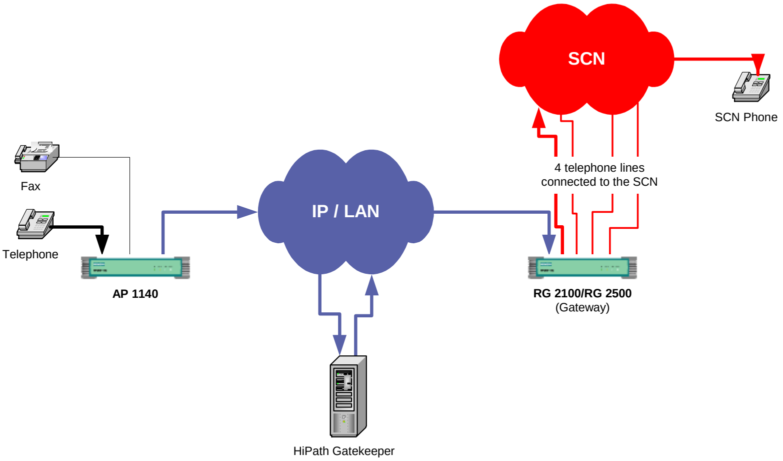
Calls Involving a SCN Gateway

The following example illustrates how a telephone/fax connected to an HiPath AP 1140 terminal and a SCN phone can communicate via a SCN gateway.

- ▶ **Phone/Fax -> HiPath AP 1140 -> RG 2100/RG 2500(Gateway) -> SCN**

A user makes a call with the phone/fax connected to an HiPath AP 1140, which in turn contacts an HiPath RG 2100/RG 2500 gateway, then reaches the corresponding SCN Phone.

A SCN user can also contact the HiPath RG 2100/RG 2500 gateway, which in turn contacts the HiPath AP 1140, then reaches the corresponding phone/fax.



Calls Without a Gatekeeper (Direct Calls)

If a FXS port of the HiPath AP 1140 or another terminal is not configured to register with a gatekeeper, you can reach this FXS port by dialing the IP address of the HiPath AP 1140 and the E.164 alias of this FXS port.

This requires a LAN H.323 endpoint that allows to dial both an IP address and an E.164 alias.

- ▶ **To make a direct call without a gatekeeper:**

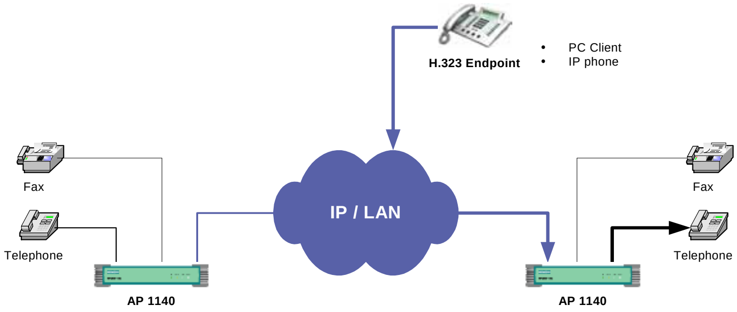
1. Dial “**” (IP address prefix).
2. Dial the numerical digits of the IP address and use the “*” for the “.” of the IP address.

3. Dial “#”, then the telephone number (E.164 alias) of the specific port you want to reach.
4. Dial “*” to terminate the IP address.

For example, let’s say you want to reach the telephone connected to Port 3 of the HiPath AP 1140 with the IP address 192.168.0.23. The phone number assigned to Port 3 of this HiPath AP 1140 is 1234. You must then dial the following digits:

```
**192*168*0*23#1234*
```

▶ **IP Address Call**



This type of dialing can only be possible if the called FXS port is not configured to register with a gatekeeper.

Using Dialing Rules

When making calls with one of the phones or faxes connected to the HiPath AP 1140, these calls follow dialing rules you have defined (see “Configuring Incoming and Outgoing Calls Parameters” on page 45 for details).

A dialing rule is a logic used to parse the digits (DTMF) received from a line (FXS port). It helps to determine if an IP address or an E.164 alias is complete.

General Dialing Rules

- The rules are applied according to a specific priority order. They are presented in this priority order.
- The dialing rules are configurable from the *Configuration* web page. Each FXS port can have its own dialing rules.
- The one digit speed dial cannot be equal to the end of dialing character.

- When the user dials a sequence that is not recognized as an E.164 alias or as the IP address prefix, an error tone is played.
- If the user dials an invalid IP address, for example "205.237.2488", an error tone is played.

Dialing Rule Priority	Description
Priority 1: Automatic speed dial	The call is automatically routed on the IP network. The destination is an E.164 alias or an H.323 ID alias. – No digit needs to be dialed in order to activate the automatic speed dial.
Priority 2: One digit speed dial	When dialing a particular digit, a new call is automatically started and routed on the IP network. The destination of the call is an E.164 alias or an H.323 ID alias. – The one digit speed dial must be from [0-9, *, #]. – The one digit speed dial must be the first digit entered. For instance, dialing *9* will start the speed dialing, while dialing *192* will not. – If the IP address prefix is recognized, this rule is not applied.
Priority 3: IP address prefix	In order to dial an IP address, a prefix must be dialed first. – Prefix consists of 1 to 4 digits from [0-9, *, #]. – Default prefix is [**]. – When the IP address prefix is recognized, the IP address dialing rules are applied. See "IP Address Specific Rules" on page 80. – When the IP address prefix is recognized, the *One digit speed dial*, *End of dialing character* and *Assume end of dialing after n digits* rules are not applied. – When the IP address prefix is recognized, the *Assume end of dialing after n seconds* rule is still applied. – In order to dial an IP address, the IP address prefix must be the first digits to be dialed. Otherwise the IP address prefix is not recognized.

Dialing Rule Priority	Description
Priority 4: End of dialing character	The user dials a particular digit to indicate that an E.164 alias is complete. – Valid characters are “*”, “#” or nothing (no end of dialing character). – If the IP address prefix is recognized, this rule is not applied. – The end of dialing character is not part of an E.164 alias. For example, if the end of dialing character is “*” and the user dials “8298749*”, a new call is started with “8298749”. – If the end of dialing character is “*”, the “#” can be dialed in an E.164 alias. – If the end of dialing character is “#”, the “*” can be dialed in an E.164 alias. – If there is no end of dialing character, both “*” and “#” can be dialed in an E.164 alias.
Priority 4: Assume end of dialing after *n* digits	An E.164 alias is considered complete after *n* digits are dialed. – Any value between 1 and 20 digits. – Default value is 20 digits. – If the IP address prefix is recognized, this rule is not applied.
Priority 4 Assume end of dialing after *n* seconds	An E.164 alias is considered complete *n* seconds after the last digit was dialed. – A value between 5 and 20 seconds. – Default value is 5 seconds. – This rule is also applied when dialing an IP address.

IP Address Specific Rules

The following rules apply when dialing an IP address.

Dialing Rule	Description
IP address prefix	See "General Dialing Rules" on page 77.
IP address dots	The dots of an IP address are dialed using "*". – This rule is applied once the IP address prefix is recognized.
Terminating an IP address	An IP address is terminated by dialing "*". Instead of dialing "*", the user can also wait *n* seconds before the IP address is considered complete. – This rule is applied once the IP address prefix is recognized. – *n*, the number of seconds, is the value of the *Assume end of dialing after n seconds* rule (see "General Dialing Rules" on page 77).
IP address time out	If the IP address is not complete *n* seconds after the last digit was dialed, a time out condition occurs. When this time out occurs, an error tone is played. – This rule is applied once the IP address start-up sequence is recognized. – *n*, the number of seconds, is the value of the *Assume end of dialing after n seconds* rule (see "General Dialing Rules" on page 77). – For example: the IP address start-up sequence is "**" and the *Assume end of dialing after n seconds* rule is set to 5 seconds. The user dials "**205" and then waits. 5 seconds later, a time out occurs and the error tone is played.

Dialing Rules Examples

The following are dialing examples that illustrate the various settings of the HiPath AP 1140.

Example 1

For this example, the following configuration is used:

- Speed dialing disabled

- IP address prefix: ******
- End of dialing character: *****
- Assume end of dialing after **7** digits
- Assume end of dialing after **5** seconds

With this configuration, if the first digit to be dialed is “*”, it is not recognized as the end of dialing character but as the first “*”of the IP address prefix. The “IP address prefix” rule has a higher priority than the “End of dialing character” rule.

▶ **Case 1: The user wants to dial 829-8749.**

1. The user dials “8298749”. When the last “9” is dialed, the E.164 alias is considered complete because 7 is the maximum number of digits for an E.164 alias.

   Complete sequence: 8298749

▶ **Case 2: The user wants to dial #245.**

1. The user dials “#245”.
2. The user dials “*”. When “*” is dialed, the E.164 alias is considered complete.

   Complete sequence: #245*

▶ **Case 3: The user wants to dial #245. The user does not know what is the end of dialing character.**

1. The user dials “#245”.
2. The user waits. 5 seconds after the last digit was dialed, the E.164 alias is considered complete.

   Complete sequence: #245

▶ **Case 4: The user wants to dial 204.236.247.67.**

1. The user dials “**” (IP address prefix).
2. The user dials “204*236*247*67*”.

   Complete sequence: **204*236*247*67*

▶ **Case 5: The user wants to dial 204.236.247.67. The user does not know that an IP address is terminated with a “*”.**

1. The user dials “**” (IP address prefix).
2. The user dials “204*236*247*67”.
3. The user waits 5 seconds. 5 seconds after the last digit was dialed, the IP address is considered complete.

Complete sequence: **204*236*247*67

▶ **Case 6: The user wants to dial 204.236.247.67.**

1. The user dials “1**”. The IP address prefix is not recognized because another digit was dialed before. Actually, this sequence is recognized as an E.164 alias equal to “1”. The second “*” is ignored.

Example 2

For this example, the following configuration is used:

- Speed dialing enabled with “*”. Speed dial alias is 1230.
- IP address prefix: **#**.
- End of dialing character: none.
- Assume end of dialing after **4** digits.
- Assume end of dialing after **5** seconds.

▶ **Case 1: The user wants to dial 2340.**

1. The user dials “2340”. When the last “0” is dialed, the E.164 alias is considered complete because 4 is the maximum number of digits for an E.164 alias.

   Complete sequence: 2340

▶ **Case 2: The user wants to dial 240.**

1. The user dials “240”.
2. Since the *End of dialing character* rule is set to none, the user must wait 5 seconds before the E.164 alias is considered complete.

   Complete sequence: 240

▶ **Case 3: The user wants to dial 1230.**

1. The user dials “*” (one digit speed dial).
2. The speed dial is activated. A new call is started with “1230”.

   Complete sequence: *

▶ **Case 4: The user wants to dial 204.236.247.67.**

1. The user dials “#” (IP address prefix).
2. The user dials “204*236*247*67*”.

   Complete sequence: #204*236*247*67*

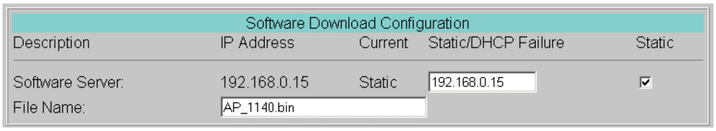
Software Upgrade

This chapter describes how to upgrade the HiPath AP 1140 software with a new version.

Setting up Software Download

The *Software Download Configuration* section of the *Configuration* web page defines the parameters for software updates.

Figure 22: Software Download Configuration Section



Software Download Configuration

Description	IP Address	Current	Static/DHCP Failure	Static
Software Server:	192.168.0.15	Static	192.168.0.15	☑
File Name:	AP_1140.bin			

The following parameters can be set:

Parameter	Definition
Software server	Server running the TFTP protocol to allow the software updates of the HiPath AP 1140. **Note:** See “Appendix A – DHCP Server Vendor Specific Information” on page 95 for more details.
File name	Name of the new software file. It can have up to 50 alphanumeric characters (a-z, A-Z, 0-9). Spaces and dots are allowed.

Downloading a New Software Version

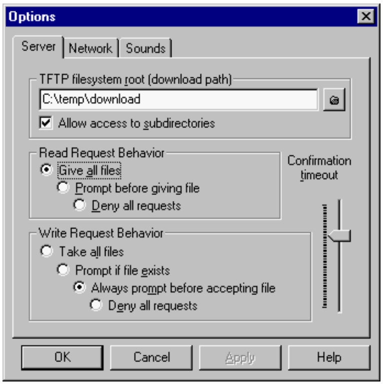
In order to download the software into the HiPath AP 1140, you must have a TFTP (Trivial File Transfer Protocol) server running on the PC designated as the software file server. This application will let you download the new software into your HiPath AP 1140.

If you don’t have a TFTP server, you can download “Pumpkin” (one of the best and fastest TFTP servers available) at http://www.klever.net/kin/pumpkin.html#technical.

1. Install the TFTP application on the PC designated as the software file server and run it.
2. From the main screen of Pumpkin, go into the *Options* menu and configure the path of the new *.bin* application file location.

3. Select *Give all files* from the *Read Request Behavior* section, then click *OK*. Leave the application running.

Figure 23: Pumpkin Options



TFTP filesystem root (download path)

C:\temp\download

☑ Allow access to subdirectories

Read Request Behavior

● Give all files

○ Prompt before giving file

○ Deny all requests

Confirmation timeout

Write Request Behavior

○ Take all files

○ Prompt if file exists

● Always prompt before accepting file

○ Deny all requests

4. From the PC, launch your Internet browser and enter the IP address of the HiPath AP 1140 you want to upgrade.

The HiPath AP 1140's configuration web pages are displayed.

5. Once on the HiPath AP 1140's web page, click the *Configuration* link in the left frame. Enter the following information when prompted:

User Name = HiPathAdm

Password = 8749Trix

These are the default values. If you have changed them (see "Changing the Password/User Name" on page 29 for more details), enter the new user name and password.

> The User Name and Password are case sensitive hence they must be entered as shown above.

6. Once on the *Configuration* screen, scroll down to the *Software Download Configuration* section and fill in the missing information if required.

7. Scroll down to the bottom of the page and click the *Update* button.

The configuration is updated, but the HiPath AP 1140 does not reboot.

8. Click the *Download* button to start the download process.

One of the two following possibilities will occur:

- The HiPath AP 1140 is in use: The software download is not processed. A warning message informs you of this situation.
- The HiPath AP 1140 is not in use: The unit goes into an updating state and becomes unusable during the download time. A message is displayed to indicate that the software download has started.

The download time varies depending on the performance of the network to which the HiPath AP 1140 is connected.

When the download process is complete, the HiPath AP 1140 will reboot automatically. This will take 10 to 20 seconds. You will then be able to access the HiPath AP 1140’s web page in order to verify that the software version has changed (displayed on the *Overview* and Configuration web pages).

Emergency Software Download Configuration Section

During the software download process, the new software file is first downloaded into the RAM of the HiPath AP 1140, then it is transferred from the RAM to the EEPROM. The HiPath AP 1140 then reboots. See section “Setting up Software Download” on page 83 for informations on how to initiate a software download.

If the transfer from the RAM to the EEPROM is suddenly interrupted, only a part of the software file is transferred to the EEPROM. Without any protection against this situation, the software file in the EEPROM is incomplete and the HiPath AP 1140 is not functional.

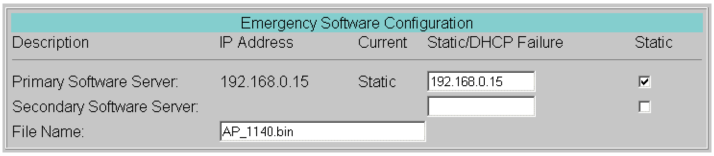
A transfer may be interrupted for the following reasons:

- An electrical shortage can interrupt the transfer of the software file from the RAM to the EEPROM.
- The user of the HiPath AP 1140 can accidentally power off the unit when the software file is being transferred from the RAM to the EEPROM.

To avoid this situation, the HiPath AP 1140 has a rescue application that automatically starts a new software download. The rescue application uses the parameters of the *Emergency Software Configuration* section in the *Configuration* web page to initiate the emergency software download.

The rescue application also sends messages to the Syslog daemon’s IP address specified in the *Syslog Daemon* field of the *IP Configuration* section.

Figure 24: Emergency Software Download



Emergency Software Configuration

Description	IP Address	Current	Static/DHCP Failure	Static
Primary Software Server:	192.168.0.15	Static	192.168.0.15	☑
Secondary Software Server:				☐
File Name:	AP_1140.bin			

The following parameters can be set:

Parameter	Definition
Primary software server	Server to contact in case the HiPath AP 1140 is interrupted while it is internally updating its software version and is now in a corrupted state. If the emergency software download fails with this IP address, for example if the primary software server cannot be reached, the IP address of the secondary software server is then used.
Secondary software server	Backup server to contact in case the HiPath AP 1140 is interrupted while internally updating its software version and is now in a corrupted state.
File name	Name of the new software file. It can have up to 50 alphanumeric characters (a-z, A-Z, 0-9). Spaces and dots are allowed.

For the IP addresses in this section, see "Appendix A – DHCP Server Vendor Specific Information" on page 95 for more details.

Using the Emergency Software Procedure

When the rescue application starts, the following steps apply:

1. The rescue application tries to initiate a software download with the primary software server.
2. If the software download fails with the primary software server, the rescue application tries to initiate a software download with the secondary software server.
3. If the software download also fails with the secondary software server, the HiPath AP 1140 idles for one (1) minute.
4. After this one (1) minute, the HiPath AP 1140 retries to initiate a software download.
5. If the software download fails again with the primary and secondary software server, the HiPath AP 1140 idles for two (2) minutes before trying to initiate a software download.

6. If the emergency software download still fails, the HiPath AP 1140 retries to initiate the software download by doubling the delay between each try up to a maximum of 16 minutes:

- first try: 1 minute delay
- second try: 2 minutes delay
- third try: 4 minutes delay
- fourth try: 8 minutes delay
- fifth try: 16 minutes delay
- sixth try: 16 minutes delay
- etc.

The rescue application will continue until the software download completes successfully.

The software download can fail if the software server cannot be reached or if the software file is not found on the software server.

Maintenance

This chapter explains how to maintain the HiPath AP 1140. It also contains a troubleshooting section that helps you find and correct the most common problems you may encounter with the HiPath AP 1140.

Warning

To prevent fire or shock hazard do not expose this unit to rain or moisture.

Caution Regarding Handling

The HiPath AP 1140 is in fact a small computer device that must be handled with some caution. This section will illustrate the basic facts regarding handling, storage and cleaning.

Location

Install the HiPath AP 1140 in a well ventilated location where it will not be exposed to high temperature or humidity.

Do not install the HiPath AP 1140 in a location which is exposed to direct sunlight or near stoves or radiators. Excessive heat could damage the internal components. See “Choosing a Suitable Location” on page 9 for more details.

Condensation

When the unit is brought into a warm environment from the cold, condensation may result which might be harmful to the unit. If this occurs, allow the unit to acclimatize for an hour before powering it.

Cleaning

To clean the HiPath AP 1140, wipe with a soft dry cloth. Do not use volatile liquids such as benzine and thinner which are harmful to the unit casing.

For resistant markings, wet a cloth with a mild detergent, wring well then wipe off. Use a dry cloth to dry the surface.

Troubleshooting

The HiPath AP 1140 is simple to install and operate, but there are some minor problems that can be experienced when it is connected to its HiPath environment. The following section will examine some of these problems and possible solutions.

> Problems encountered by the HiPath AP 1140 are listed in a Syslog message. You can see this message with the Syslog daemon.

Solving General Operation Problems

Unit does not operate – All LEDs are OFF

Power is not fed to the unit. Check that:

- The power cord is connected to the AC socket.
- The power connector is fully inserted into the HiPath AP 1140 power socket.

Dial tone is not received at the telephone

If the *Power* LED is on and the In Use LED is off, the connection between the phone and the HiPath AP 1140 is not working properly. Check that:

- Both ends of the RJ-11 analog line cable are securely connected.
- The In Use LED lights up when the phone is off hook.

Impossible to make a call

If the following happens:

- Dial tone present.
- *Power* LED on.
- In Use LED lights up when the phone is off hook.
- *LAN* LED on.

Network communication is not working. Check that:

- The LAN cable is securely connected to the HiPath AP 1140 and to the network connector.
- You did not connect a crossover network cable.

Impossible to make a call to a destination

If the following happens:

- Dial tone present.
- *Power* LED on.
- In Use LED lights up when the phone goes off hook.
- *LAN* LED on.

Configurable parameters of the HiPath AP 1140 are not set properly.

- Refer to the previous chapters of this manual for a complete description of the configurable parameters of the HiPath AP 1140.

“Poor line condition” error during a fax transmission

The analog transmission between the fax machine and the HiPath AP 1140 is flaky, preventing the fax transmission to terminate properly. This problem is known to occur with some fax machines and it can also occur with a few fax modems. To remedy the problem:

- In the *Configuration* web page, access the *FXS Port* sections and set the *Input sound level* and *Output sound level* to **-6 dB**. If this still does not solve the problem, try the **+6 dB** value. For more information, refer to “Configuring Incoming and Outgoing Calls Parameters” on page 45.

Solving Web Interface Problems

The Web browser cannot access the HiPath AP 1140 over the network

Check that:

- The IP information for the HiPath AP 1140 is correctly configured.

Some of the web interface is not displayed in the Web browser after downloading

This is probably due to large amounts of traffic on the network. Either reload the web interface or click in the part of the interface that has not displayed and select the reload frame option in your Web browser.

“URL not found” message is displayed when trying to access the web interface

The Web browser cannot access the HiPath AP 1140’s web interface. Check that:

- You have the proper IP address.
- You have used the port 8085.
- The LAN cable is securely connected to the HiPath AP 1140 and to the network connector.
- You did not connect a crossover network cable.

The HiPath AP 1140 information shown on the web interface does not refresh automatically

You may need to make a small change to your Web browser so that it always downloads the latest version of a web page from the web interface.

▶ **To do this for Netscape Navigator 4.7:**

1. Start Netscape Navigator.
2. From the *Edit* menu, select *Preferences*.

   The *Preferences* dialog box opens.
3. Select the *Advanced* folder, then the *Cache* option.
4. Check the *Every Time* checkbox.
5. Click *OK*.

▶ **To do this for Microsoft Internet Explorer 5.0:**

1. Start Microsoft Internet Explorer.
2. From the *Tools* menu, select *Internet Options*.

   The *Internet Options* dialog box opens.
3. In the *General* tab, and in the T*emporary Internet Files* section, click the *Settings* button.
4. Check the *Every visit to the page* checkbox.
5. Click *OK*.

Solving Software Upgrade Problems

An error occurs when the HiPath AP 1140 attempts to communicate with the software server

There could be a number of reasons for this:

- The file specified in the upgrade command does not exist or is in a different directory than the one given.
  - Check the file name and its location.
  - Make sure that the software server (TFTP) is running and is properly configured.
- The IP address of the software server is not the correct one.
  - Check the given IP address.
  - Check the IP port.

An error occurs when the HiPath AP 1140 attempts to transfer the file

There could be a number of reasons for this:

- The Ethernet cable has become disconnected from the HiPath AP 1140 or the PC running the file transfer. Reconnect the cable and start again.
- Power to the HiPath AP 1140 has been disrupted during the file transfer. Check the power connection to the HiPath AP 1140 and start again.
- An incorrect file is being specified and transferred to the HiPath AP 1140. Check the file name and start again.

Appendix A – DHCP Server Vendor Specific Information

The HiPath AP 1140 uses a DHCP server to receive the IP addresses it needs to work properly. This Appendix assumes that you know how to set up and use a DHCP server. If not, ask your network administrator to set up DHCP-related variables.

Configuring the DHCP Server

DHCP servers generally allocate a range of IP addresses for use on a network and reserve IP addresses for specific devices using a unique identifier for each device. The HiPath AP 1140 unique identifier is its media access control (MAC) address. The MAC address appears on the label located on the bottom side of the unit. It can also be found in the web page. Siemens AG recommends that you reserve an IP address for each HiPath AP 1140 on the network.

In addition to the IP address, the DHCP server can set other configurable options within the HiPath AP 1140. The unit expects to receive its network configuration from the DHCP server via the vendor specific codes.

Siemens AG recommends that you use a Windows 2000- or Unix-based DHCP server. If you run Windows NT 4.0 and use the built-in Microsoft DHCP Server, you must use the Site Specific option instead of Vendor Specific option.

Network Configuration

Configure the DHCP server to set the following network options:

Option	Description	Type	Data Format	Example
Subnet Mask	Specifies subnet configuration	001	xxx.xxx.xxx.xxx	255.255.255.0
Routers	List of routers on your network	003	Array of IP Addresses	192.168.10.1 192.168.10.2
DNS Servers	List of DNS servers on your network	006	Array of IP Addresses	192.168.10.11 192.168.10.12

Creating Vendor Specific Information

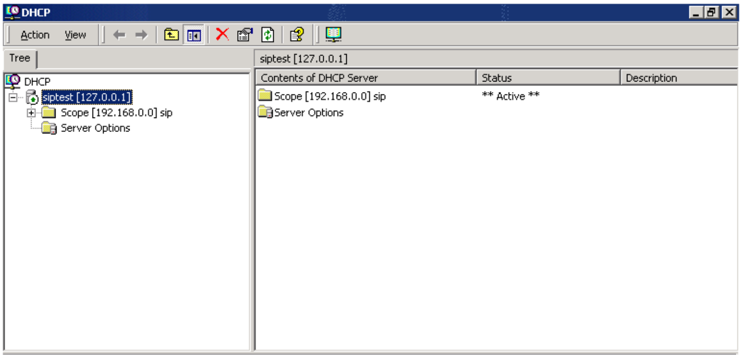
The following section describes how to set Vendor specific information in a Windows 2000-based DHCP server. How to create vendor specific information differs from one DHCP server program to another.

▶ To create vendor specific information:

1. In *Start/Program/Administrative Tools*, select *DHCP*.

   The following window opens.

Figure 25: DHCP Manager



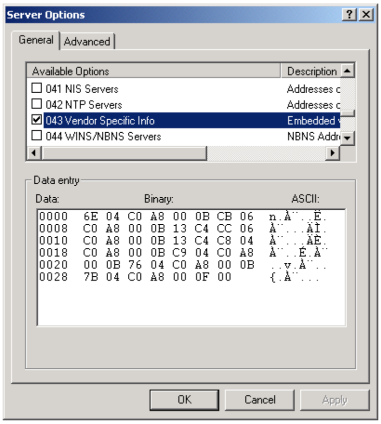
siptest [127.0.0.1]

- DHCP
  - siptest [127.0.0.1]
    - Scope [192.168.0.0] sip
    - Server Options

Contents of DHCP Server	Status	Description
Scope [192.168.0.0] sip	** Active **	
Server Options		

2. In the tree list on the left, select *Server Options*.
3. In the *Action* menu, select the *Configure Options* task.
4. Scroll down the list in the window that opens and select the *043 Vendor Specific Info* option.

Figure 26: Vendor Specific Information



Available Options	Description
☐ 041 NIS Servers	Addresses c
☐ 042 NTP Servers	Addresses c
☑ 043 Vendor Specific Info	Embedded v
☐ 044 WINS/NBNS Servers	NBNS Addr

```
Data:            Binary:                    ASCII:
0000   6E 04 C0 A8 00 0B CB 06   n.À¨..Ë.
0008   C0 A8 00 0B 13 C4 CC 06   À¨...ÄÌ.
0010   C0 A8 00 0B 13 C4 C8 04   À¨...ÄÈ.
0018   C0 A8 00 0B C9 04 C0 A8   À¨..É.À¨
0020   00 0B 76 04 C0 A8 00 0B   ..v.À¨..
0028   7B 04 C0 A8 00 0F 00      {.À¨...
```

The *Server Options* window now lists the current Vendor Specific information set in the DHCP server.

5. Click in the last line entered, then type in the Vendor Specific Information you want to add.

A new line will be automatically created. Use one line for each Vendor Specific information you want to add. The information must be defined in binary (hexadecimal) format. You can enter a maximum of 255 characters per line. See "Entering IP Addresses' on page 98 for more details on the syntax to use.

6. When you are done, click *OK*.

Firewall Information: the HiPath AP 1140 uses UDP port 5060.

The following table lists the HiPath AP 1140 codes for Vendor Specific information:

Item of Information	**Vendor Specific Code**	
	Decimal	**Hexadecimal**
Syslog	110	6E
Standard gatekeeper	111	6F
HiPath gatekeeper 1	112	70
HiPath gatekeeper 2	113	71
HiPath gatekeeper 3	114	72
HiPath gatekeeper 4	115	73
HiPath gatekeeper 5	116	74
Software server	117	75
Emergency Primary software server	118	76
Emergency Secondary software server	119	77

Entering IP Addresses

IP addresses must be entered in hexadecimal. There are two formats of address string:

- Long: Has a size of 6 hexadecimal characters and includes the IP address and port.
- Short: Has a size of 4 hexadecimal characters and includes only the IP address. In this case, the default port is used.

Variable	Valid Range	Typical Value	Note
IP Address	Any valid IP address	192.168.0.2	N/A
Port	1 - 32,768	162	Not present in the format with dimension 4.

If the DHCP request fails or the address is not in the vendor specific codes, the following applies:

1. If the DHCP value already in the configuration is valid, it is kept.
2. If not, the static value is used if valid.
3. If not, the default value is used.

Example

The following example shows how to enter the Syslog IP address 192.168.0.10 (with the default port used) and the same address at port 2545. The Vendor Specific Code is 110.

Figure 27: Example – Short Address String

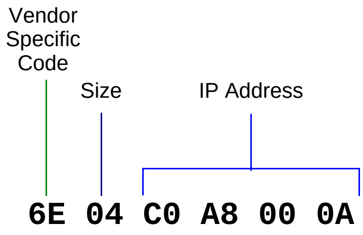
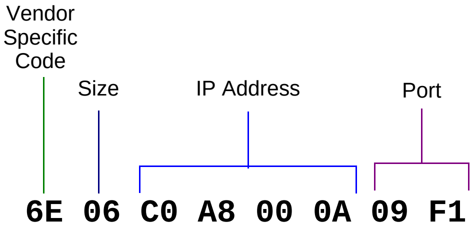


Figure 28: Example – Long Address String



Appendix B – Country Specific Parameters

The following parameters differ depending on the country you are in. Note that the *On – Off* sequence is read as follows:

– **1.0** – 0.85 means that the sequence is 1.0 second On and 0.85 second Off. The bold number always refers to the *On* sequence.

Austria

The following parameters apply if you have selected Austria as location.

Parameter	**Value**	**On** – Off **Sequence (s)**	**Elect. Levels**
Dial Tone	450 Hz	**1.0** – 0.85	-20 dBm
Busy Tone	450 Hz	**0.45** – 0.45	-20 dBm
Ringing Tone	450 Hz	**1.0** – 4.0	-20 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.33 0.33 **0.33** – 1.0	-20 dBm
Ring	65 VRMS, 50 Hz	**1** – 5	
Impedance	Z_R = 270 Ω + 750 Ω // 150 nF		
Tbrl-Impedance	Z_N = 600 Ω		
FXS Line Attenuation (Input)			+3 dBr
FXS Line Attenuation (Output)			-10 dBr

France

The following parameters apply if you have selected France as location.

Parameter	**Value**	**On** – Off **Sequence (s)**	**Elect. Levels**
Dial Tone	330 Hz	CONTINUOUS	-16.9 dBm
Busy Tone	440 Hz	**0.5** – 0.5	-19.9 dBm
Ringing Tone	440 Hz	**1.5** – 3.5	-19.9 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.33 0.33 **0.33** – 1.0	-19.9 dBm
Ring	75 VRMS, 50 Hz	**1.5** – 3.5	

Parameter	Value	**On** – Off **Sequence (s)**	**Elect. Levels**
Impedance	Z_R = 215 Ω + 1000 Ω // 137 nF		
Tbrl-Impedance	Z_N = 600 Ω		
FXS Line Attenuation (Input)			-1.9 dBr
FXS Line Attenuation (Output)			-8.9 dBr

Germany

The following parameters apply if you have selected Germany as location. Germany 1 and Germany 2 calibration were asked for by Siemens AG. Both calibrations are present in the ETSI PBX standard :

“ES 201 168 Corporate Networks (CN) Transmission characteristics of digital Private Branch eXchanges (PBXs)”.

In this standard, Germany 1 is defined as an option while Germany 2 is the default configuration.

Parameter	Value	**On** – Off **Sequence (s)**	**Elect. Levels**
Dial Tone	425 Hz	**0.2** – 0.3 - **0.2** – 0.3 - **0.2** – 0.8	-16 dBm
Busy Tone	425 Hz	**0.17** – 0.43	-16 dBm
Ringing Tone	425 Hz	**1.0** – 4.0	-16 dBm
Special Information Tone	425 Hz	**0.17** – 0.43	-16 dBm
Ring	75 VRMS, 25 Hz	**1** – 4	
Impedance	Z_R = 220 Ω + 820 Ω // 115 nF		
Tbrl-Impedance	Z_N = 220 Ω + 820 Ω // 115 nF		
FXS Line Attenuation (Input)			+3 dBr
FXS Line Attenuation (Output)			-10 dBr

Parameter	Value	**On** – Off **Sequence (s)**	**Elect. Levels**
Dial Tone	425 Hz	**0.2** – 0.3 - **0.2** – 0.3 - **0.2** – 0.8	-13 dBm
Busy Tone	425 Hz	**0.17** – 0.43	-13 dBm
Ringing Tone	425 Hz	**1.0** – 4.0	-13 dBm
Ring	75 VRMS, 25 Hz	**1** – 4	

Parameter	Value	**On** – Off **Sequence (s)**	Elect. Levels
Impedance	Z_R = 220 Ω + 820 Ω // 115 nF		
Tbrl-Impedance	Z_N = 220 Ω + 820 Ω // 115 nF		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-7 dBr

Great Britain

The following parameters apply if you have selected Great Britain as location.

Parameter	Value	**On** – Off **Sequence (s)**	Elect. Levels
Dial Tone	350+440 Hz	CONTINUOUS	-19 dBm
Busy Tone	400 Hz	**0.375** – 0.375	-19 dBm
Ringing Tone	400+450 Hz	**0.4** – 0.2 - **0.4** – 2.0 - **0.35** – 0.22 followed by **0.4** – 0.2 - **0.4** – 2.0	-19 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.33 0.33 **0.33** – 1.0	-19 dBm
Ring	62 VRMS, 25 Hz	**1.0** – 4.0	
Impedance	Z_R = 300 Ω + 1000 Ω // 220 nF		
Tbrl-impedance	Z_N = 370 Ω + 620 Ω // 310 nF		
FXS Line Attenuation (Input)			+3 dBr
FXS Line Attenuation (Output)			-9 dBrr

Italy

The following parameters apply if you have selected Italy as location.

Parameter	Value	**On** – Off **Sequence (s)**	Elect. Levels
Dial Tone	425+350 Hz	CONTINUOUS	-10 dBm
Busy Tone	425 Hz	**0.5** – 0.5	-13 dBm
Ringing Tone	425 Hz	**1.0** – 4.0	-13 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.33 0.33 **0.33** – 1.0	-20 dBm

Parameter	**Value**	**On** – Off **Sequence (s)**	**Elect. Levels**
Ring	75 VRMS, 25 Hz	**1.0** – 4.0	
Impedance	Z_R = 180 Ω + 630 Ω // 60 nF		
Tbrl-impedance	Z_N = 750 Ω // 18 nF		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-7 dBr

North America

The following parameters apply if you have selected North America as location.

Parameter	**Value**	**On** – Off **Sequence (s)**	**Elect. Levels (Level per frequency)**
Dial Tone	350+440 Hz	CONTINUOUS	-17 dBm
Busy Tone	480+620 Hz	**0.5** – 0.5	-21 dBm
Ringing Tone	440+480 Hz	**2.0** – 4.0	-16 dBm
Intercept Tone	440 Hz 620 Hz	**0.25** – 0.25 **0.25** – 0.25	-14 dBm
Ring	70 VRMS, 20 Hz	**2.0** – 4.0	
Impedance	Z_R = 600 Ω		
Tbrl-Impedance	Z_N = 600 Ω		
FXS Line Attenuation (Input)			+3 dBr
FXS Line Attenuation (Output)			-3 dBr

Parameter	**Value**	**On** – Off **Sequence (s)**	**Elect. Levels (Level per frequency)**
Dial Tone	350+440 Hz	CONTINUOUS	-17 dBm
Busy Tone	480+620 Hz	**0.5** – 0.5	-21 dBm
Ringing Tone	440+480 Hz	**2.0** – 4.0	-16 dBm
Intercept Tone	440 Hz 620 Hz	**0.25** – 0.25 **0.25** – 0.25	-14 dBm
Ring	70 VRMS, 20 Hz	**2.0** – 4.0	

Parameter	Value	**On** – Off **Sequence (s)**	Elect. Levels (Level per frequency)
Impedance	Z_R = 600 Ω		
Tbrl-Impedance	Z_N = 350 Ω + 1000 Ω // 210 nF		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			0 dBr

Spain

The following parameters apply if you have selected Spain as location.

Parameter	Value	**On** – Off **Sequence (s)**	Elect. Levels
Dial Tone	425 Hz	**0.2** – 0.3 - **0.2** – 0.3 - **0.2** – 0.8	-10 dBm
Busy Tone	425 Hz	**0.2** – 0.2	-13 dBm
Ringing Tone	425 Hz	**1.5** – 3.0	-13 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.33 0.33 **0.33** – 1.0	-20 dBm
Ring	75 VRMS, 25 Hz	**1.5** – 3.0	
Impedance	Z_R = 220 Ω + 820 Ω // 120 nF		
Tbrl-Impedance	Z_N = 220 Ω + 820 Ω // 120 nF		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-7 dBr

Switzerland

The following parameters apply if you have selected Switzerland as location.

Parameter	Value	**On** – Off **Sequence (s)**	Elect. Levels
Dial Tone	425 Hz	CONTINUOUS	-8 dBm
Busy Tone	425 Hz	**0.5** – 0.5	-13 dBm
Ringing Tone	425 Hz	**1.0** – 4.0	-13 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.33 0.33 **0.33** – 1.0	-13 dBm

Parameter	Value	**On** – Off **Sequence (s)**	Elect. Levels
Ring	70 VRMS, 25 Hz	**1.0** – 4.0	
Impedance	Z_R = 220 Ω + 820 Ω // 115 nF		
Tbrl-impedance	Z_N = 220 Ω + 820 Ω // 115 nF		
FXS Line Attenuation (Input)			-0 dBr
FXS Line Attenuation (Output)			-6.5 dBr

Europe

The following parameters apply if you have selected Europe as location.

Parameter	Value	**On –** Off **Sequence (s)**	Elect. Levels
Dial Tone	425 Hz	CONTINUOUS	-14 dBm
Busy Tone	425 Hz	**0.5** – 0.5	-14 dBm
Ringing Tone	425 Hz	**1.0** – 4.0	-14 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	0.33 0.33 **0.33** – 1.0	-20 dBm
Ring	AC: 4565 VRMS, 25 Hz DC: 15 Vdc	**1.0** – 4.0	
Impedance	Z_R = 270 Ω + 750 Ω // 150 nF		
Tbrl-Impedance	Z_N =270 Ω + 750 Ω // 150 nF		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-7 dBr

Appendix C – Safety & EMI Certifications

This Appendix lists the various Safety and EMI certifications of the HiPath AP 1140.

Safety & EMI Certifications Supported

The HiPath AP 1140 has received the following Safety & EMI Certifications:

> The Safety and EMI Certifications of the HiPath AP 1140 are printed on a sticker located on the bottom of the unit.

- ; FCC Part 68 subpart D
-
- UL and UL-C
- CSA and CSA-US

Disclaimers

Federal Communications Commission (FCC) Part 15

This equipment has been tested and found to comply with the limits for Class A Digital Device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

> Any changes or modifications not expressly approved by Siemens AG could void the user’s authority to operate the equipment.

Federal Communications Commission (FCC) Part 68

This equipment complies with Part 68 of the FCC Rules. On the underside of this equipment is a label that contains, among other information, the FCC Registration Number, Ringer Equivalence Number (REN) and USOC jack type for this equipment. You must, upon request, provide this information to your telephone company.

The REN is useful to determine the quantity of devices you may connect to your telephone line and still have all of those devices ring when your telephone number is called. In most, but not all areas, the sum of the REN's of all devices connected to one line should not exceed five (5.0). To be certain of the number of devices you may connect to your line, as determined by the REN, you should contact your telephone company to determine the maximum REN for your calling area. If your telephone equipment causes harm to the telephone network, the Telephone Company may discontinue your service temporarily. If possible, they will notify you in advance, but if advance notice is not practical, you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC.

Your telephone company may make changes in its facilities, equipment, operations or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with this telephone equipment, please contact Siemens AG for information on obtain service or repairs. The telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.

This equipment may not be used on coin service provided by the telephone company.

Connection to party lines is subject to state tariffs.

INSTALLATION

This device is equipped with an USOC RJ-11C connector.

Industry Canada

The Industry Canada Label identifies certified equipment. This certification means that the equipment meets telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

> ! Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

> ℹ The Ringer Equivalence Number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Number of all the devices does not exceed 5.

CE Mark

The HiPath AP 1140 gateway complies with the EMC and low voltage Directives.

Appendix D – Glossary

10 BaseT

An Ethernet local area network which works on twisted pair wiring.

100 BaseT

A newer version of Ethernet that operates at 10 times the speed of a 10 BaseT Ethernet.

A-Law

The ITU-T companding standard used in the conversion between analog and digital signals in PCM (Pulse Code Modulation) systems. A-law is used primarily in European telephone networks and contrasts with the North American mu (µ)-law standard. See also *mu (µ)-law*.

Area Code (AC)

The preliminary digits a user must dial to be connected to a particular outgoing trunk group or line. In North America, an Area Code has three (3) digits and is used with a NXX (office code) number. For example, in the North American telephone number *561-955-1212*, the numbers are defined as follows:

No.	Description
561	Area Code, corresponding to a geographical zone in a non-LNP (Local Number Portability) network.
955	NXX (office code), which corresponds to a specific area such as a city region.
1212	Unique number to reach a specific destination.

Outside North America, the Area Code may have any number of digits, depending on the national telecommunication regulation of the country. In France, for instance, the numbering terminology is defined as *xZABPQ 12 34*, where:

No.	Description
x	Operator forwarding the call. This prefix can be made of 4 digits.
Z	Geographical (regional) zone of the number (in France, there are 5 zones). It has two (2) digits.

No.	Description
ABPQ	First 4 digits corresponding to a local zone defined by central offices.
12 34	Unique number to reach a specific destination.

In this context, the Area Code corresponds to the *Z* portion of the numbering plan. Since virtually every country has a different dialing plan nomenclature, it is recommended to identify the equivalent of an Area Code for the location of your device.

Battery feed, Over-voltage protection, Ringing, Signaling, Coding, Hybrid, and Testing (BORSCHT)

A group of functions provided to an analog line from a line circuit of a digital central office switch.

Country Code (CC)

In international direct telephone dialing, a code that consists of 1-, 2-, or 3-digit numbers in which the first digit designates the region and succeeding digits, if any, designate the country.

Custom Local Area Signaling Services (CLASS)

One of an identified group of network-provided enhanced services. Note: A CLASS group for a given network usually includes several enhanced service offerings, such as incoming-call identification, call trace, call blocking, automatic return of the most recent incoming call, call redial, and selective forwarding and programming to permit distinctive ringing for incoming calls.

Digital Signal Processor (DSP)

Specialized computer chip designed to perform speedy and complex operations on digitized waveforms. Useful in processing sound (like voice phone calls) and video.

Domain Name Server (DNS)

Internet service that translates domain names into IP addresses. To use a domain name, a DNS service must translate the name into the corresponding IP address. For instance, the domain name *www.example.com* might translate to 198.105.232.4.

Dual-Tone Multi-Frequency (DTMF)

In telephone systems, multi-frequency signaling in which a standard set combinations of two specific voice band frequencies, one from a group of four low frequencies and the other from a group of four higher frequencies, are used. Although some military telephones have 16 keys, telephones using DTMF usually have 12 keys. Each key corresponds to a different pair of frequencies. Each pair of frequencies corresponds to one of the ten decimal digits, or to the symbol “#” or “*”, the “*” being reserved for special purposes.

Dynamic Host Configuration Protocol (DHCP)

TCP/IP protocol that enables PCs and workstations to get temporary or permanent IP addresses (out of a pool) from centrally-administered servers.

Electronically Erasable Programmable Read Only Memory (EEPROM)

A read only memory device that can be erased and reprogrammed. Typically, it is reprogrammed electronically (not electromagnetically) with ultraviolet light.

Erasable Programmable Read Only Memory (EPROM)

A special type of memory that retains its contents until it is exposed to ultraviolet light. The ultraviolet light clears its contents, making it possible to reprogram the memory. To write to and erase an EPROM, you need a special device called a PROM programmer or PROM burner.

Federal Communications Commission (FCC)

U.S. government regulatory body for radio, television, and interstate telecommunications services and international services originating in the United States.

Foreign Exchange Service/Station (FXS)

A network-provided service in which a telephone in a given local exchange area is connected, via a private line, to a central office in another, i.e., “foreign”, exchange, rather than the local exchange area’s central office. A FXS line is normally connected to a standard telephone, fax or modem.

G.711

ITU-T recommendation for an algorithm designed to transmit and receive A-law PCM (Pulse Code Modulation) voice at digital bit rates of 48, 56, and 64 kbps. It is used for digital telephone sets on digital PBX and ISDN channels.

G.723.1

A Codec that provides the greatest compression, 5.3 kbps or 6.3 kbps; typically specified for multimedia applications such as H.323 videoconferencing.

Gatekeeper

A gatekeeper identifies, controls, counts, and supervises the traffic or flow through the network. It also provides functions such as terminal and gateway registration, address resolution, band-width control, and admission control.

Gateway

A device linking two different types of networks that use different protocols (for example, between the packet network and the Public Switched Telephone Network).

H.323

An umbrella standard for audio/video conferencing over unreliable networks; architecture and procedures are covered by this standard; H.323 relies on H.225 and H.245.

Integrated Services Digital Network (ISDN)

An international telecommunications network, based on a set of communications standards, for digital transmission of voice, video, and data over WANs. ISDN interfaces also provide LAN connections and remote access capability. ISDN has two types of service: BRI (basic rate interface) and PRI (primary rate interface).

International Telecommunication Union (ITU)

Organization based in Geneva, Switzerland, that is the most important telecom standards-setting body in the world.

Internet Protocol (IP)

The IP protocol is a standard describing software that keeps track of the Internet's addresses for different nodes, routes outgoing messages, and recognises incoming messages.

Jitter

1. A distortion caused by the variation of a signal from its references which can cause data transmission errors, particularly at high speeds.
2. Variations in amplitude, time, frequency or phase.

Light Emitting Diode (LED)

A semiconductor diode that emits light when a current is passed through it.

Local Area Network (LAN)

Data-only communications network confined to a limited geographic area, with moderate to high data rates. See also *WAN*.

Media Access Control (MAC) Address

A layer 2 address, 6 bytes long, associated with a particular network device; used to identify devices in a network; also called hardware or physical address.

Mu (µ)-Law

The PCM (Pulse Code Modulation) voice coding and companding standard used in Japan and North America. See also *A-Law*.

Network

A group of computers, terminals, and other devices and the hardware and software that enable them to exchange data and share resources over short or long distances. A network can consist of any combination of local area networks (LAN) or wide area networks (WAN).

Off-hook

A line condition caused when a telephone handset is removed from its cradle.

On-hook

A line condition caused when a telephone handset is resting in its cradle.

Packet

Includes three principal elements: control information (such as destination, origin, length of packet), data to be transmitted, and error detection. The structure of a packet depends on the protocol.

Plain Old Telephone System (POTS)

Standard telephone service used by most residential locations; basic service supplying standard single line telephones, telephone lines, and access to the public switched network.

Port

Network access point, the identifier used to distinguish among multiple simultaneous connections to a host.

Private Branch Exchange (PBX)

A small to medium sized telephone system and switch that provides communications between onsite telephones and exterior communications networks.

Programmable Read-Only Memory (PROM)

A memory chip where data is written only once as it remains there forever. Unlike RAM, PROMs retain their contents when the computer is turned off.

Progress Message

The Progress message may be sent by an endpoint or Gatekeeper to indicate the progress of a call in the event of interworking with the SCN. This may be used to merely indicate that a Gateway in the call is interworking with the SCN or to indicate the presence of in-band information.

Protocol

A formal set of rules developed by international standards bodies, LAN equipment vendors, or groups governing the format, control, and timing of network communications. A set of conventions dealing with transmissions between two systems. Typically defines how to implement a group of services in one or two layers of the OSI reference model. Protocols can describe low-level details of machine-to-machine interfaces or high-level exchanges between allocation programs.

Public Switched Telephone Network (PSTN)

The local telephone company network that carries voice data over analog telephone lines.

Real Time Control Protocol (RTCP)

RTCP is the control protocol designed to work in conjunction with RTP. It is standardized in RFC 1889 and 1890. In an RTP session, participants periodically send RTCP packets to convey feedback on quality of data delivery and information of membership.

Ringer Equivalence Number (REN)

A number that represents the ringer loading effect on a line. Note: A ringer equivalency number of 1 represents the loading effect of a single traditional telephone set ringing circuit. Modern telephone instruments may have a REN lower than 1. The total REN expresses the total loading effect of the subscriber's equipment on the central office ringing current generator. The service provider usually sets a limit, e.g., 3, 4, or 5 (representing "extension," i.e., parallel-connected telephones), to the total REN on a subscriber's loop.

Router

A specialized switching device that allows customers to link different geographically dispersed local area networks and computer systems. This is achieved even though it encompasses different types of traffic under different protocols, creating a single, more efficient, enterprise-wide network.

Server

A computer or device on a network that works in conjunction with a client to perform some operation, for example a Windows NT Server.

Subnet

An efficient means of splitting packets into two fields to separate packets for local destinations from packets for remote destinations in TCP/IP networks.

Switched Circuit Network (SCN)

A communication network, such as the public switched telephone network, in which any user may be connected to any other user through the use of message, circuit, or packet switching and control devices.

T.38

An ITU-T Recommendation for Real-time fax over IP. T.38 addresses IP fax transmissions for IP-enabled fax devices and fax gateways, defining the translation of T.30 fax signals and Internet Fax Protocols (IFP) packets.

Telephony

The science of translating sound into electrical signals, transmitting them, and then converting them back into sound.

Terminal

Device capable of sending or receiving data over a data communications channel.

Transmission Control Protocol/Internet Protocol (TCP/IP)

A suite of communications protocols developed by the Department of Defense in the 1970s that connects hosts on the Internet and provides the standards for transmitting data over networks.

Trivial File Transfer Protocol (TFTP)

A simplified version of FTP that transfers files but does not provide password protection, provide directory capability, or allow transmission of multiple files with one command.

User Datagram Protocol (UDP)

An efficient but unreliable, connectionless protocol that is layered over IP, as is TCP. Application programs are needed to supplement the protocol to provide error processing and retransmission of data. UDP is an OSI layer 4 protocol.

Voice Over IP (VoIP)

The technology used to transmit voice conversations over a data network using the Internet Protocol. Such data network may be the Internet or a corporate Intranet.

Wide Area Network (WAN)

A large (geographically dispersed) network, usually constructed with serial lines, that covers a large geographic area. A WAN connects LANs using transmission lines provided by a common carrier.

Numerics

10 BaseT 5, 16, 111
100 BaseT 5, 16, 111
802.1q, setting 58

A

acronyms vi
advanced debug 69
A-Law 47, 111
analog modem, feature 2
area code 111
AutoDiscovery feature 3

B

Bypass, System Failure 3, 68

C

call
  dialing rule 77
  direct 33, 76
  examples 80
  forwarding a 53
  involving a SCN gateway 76
  involving a terminal and an H.323 endpoint 74
  involving another terminal 74
  IP address 77
caller ID feature 3
Change Password/User Name web page 29
changing
  password 29
  user name 29
Configuration web page
  accessing 19
  Bypass Activation 68
  content frame 19
  definition 17
  Emergency Software Download 85
  FXS Port sections 45
  Gatekeeper configuration 33
  Geographical configuration 62
  Hardware configuration 67
  IP configuration 27
  menu frame 18
  QoS
    802.1q 58
    Differentiated Service 56
  resetting 22
  SNTP configuration 66
  Software Download configuration 83
configuring the software
  IP addresses 23
  subnet mask 23
connectors
  Bypass 5
  Default Settings 5
  Ethernet 5
  Phones/Faxes 5
  Power 5
country
  setting 62
  specific parameters 101

D

debug, advanced 69
default router, setting 27
Default Settings switch 5
  definition 10
  using 10
DHCP server
  definition 113
  requirement 9
  setting IP address 28
  vendor specific codes 95
dialing
  examples 80
  IP address call 77
  rules
    general 77
    IP address specific 80
Differentiated Service, setting 56
DNS 112
download software 83
DTMF 52, 112

E

Emergency Software Download
  IP address of server 85
  procedure 86

F

FastConnect feature 2
fax interface, feature 2
features
  analog modem 2
  AutoDiscovery 3
  call transfer 3
  caller ID 3
  FastConnect 2
  fax interface 2
  FXS ports 2
  out of band DTMF 3
  PhoneMail support 2
  Progress message 3
  RTCP 3
  system failure bypass 3
frames
  content 19
  menu 18
FXS port
  accept IP Network to Phone/Fax call 52
  accept Phone/fax to IP Network call 49
  assume end of dialing after n digits 51
  assume end of dialing after n seconds 52
  call forward
    busy 53

        no answer 53
        unconditional 53
    DTMF Tone detection duration 52
    DTMF Tone generation duration 52
    E.164 alias 46
    end of dialing character 51
    feature 2
    input sound level 47
    IP address prefix 50
    jitter buffer protection 48
    output sound level 47
    setting 45
    silence detection/suppression level 48
    speed dialing 49
    voice coding algorithm 47

G

G.711 47, 113
G.723.1 47, 113
gatekeeper
    configuration 33
    H.323 ID alias 34
    IP address 33
    IP address of HiPath 34
    lightweight registration 35, 39
    registration logic
        examples 40
        lightweight registration 39
        messages exchanged 36
        no gatekeeper registration 35
        registration 37
    retry time 35
    type 34
gateway 114
geographical configuration
    country 62
    custom time zone 62
    predefined time zone 62
    time zone 62

H

H.323 114
hardware
    cleaning 89
    condensation 89
    front indicators 4
    installing 15
    installing for the first time 10
    proper location 89
    rear connections 5

I

indicators of the hardware 4
input sound level, setting 47
installing
    hardware 15
    hardware for the first time 10
IP address
    default router 27
    default settings switch 11
    DHCP server 28
    dialing 77
    DNS, primary 27
    DNS, secondary 27
    emergency software server 86
    finding assigned
        with DHCP Server 15
        with Syslog daemon 14
    gatekeeper 33
    HiPath gatekeepers 34
    of unit 27
    SNTP server 66
    software server 83
    subnet mask 27
    syslog daemon 28
IP configuration 27

J

jitter buffer protection, setting 48
jitter, definition 114

L

LED
    behavior in download mode 7
    In Use 6
    interpreting 6
    LAN 6
    Power 6
lightweight registration, with a gatekeeper 35
local IP address, setting 27

M

MAC Address 115
messages to Syslog daemon, setting 28
Mu (µ)-Law 47, 115

O

off-hook 115
on-hook 115
out of band DTMF feature 3
output sound level, setting 47

P

password
    changing 29
    default 30, 31
PhoneMail support 2
port 115
primary DNS, setting 27
Progress message 3, 116

Q

QoS
  802.1q 58
  Differentiated Service 56

R

RAM Check 67
rear connections 5
requirements 9
restarting the unit 22
ROM Check 68
RTCP, feature 3

S

Safety & EMI Certifications
  CE Mark 109
  FCC Part 15 107
  FCC Part 68 107
  Industry Canada 108
secondary DNS, setting 27
setting
  default router 27
  DHCP server IP address 28
  FXS ports 45
  input sound level 47
  jitter buffer protection 48
  local IP address 27
  messages to Syslog daemon 28
  output sound level 47
  primary DNS 27
  secondary DNS 27
  silence detection/suppression level 48
  subnet mask 27
  Syslog daemon 28
  Syslog debug messages 28
  voice coding algorithm 47
silence detection/suppression level, setting 48
site, selecting for unit 9
software download
  default IP address 11
  initiating 83
  IP address of server 83
subnet mask
  default IP address 11
  setting 27
subnet mask, configuring 23
Syslog daemon
  default IP address 11
  enabling messages 28
  enabling messages to 28
  requirement 9
  setting IP address of 28
  using 28
Syslog debug messages, setting 28
System Failure Bypass, definition 68

T

T.38 47, 117
TCP/IP 117
TFTP server 9, 83, 117
time zone, selecting 62
troubleshooting
  all LED’s are off 90
  cannot make a call 90
  cannot make a call to a destination 91
  dial tone is not received at the telephone 90
  solving general operation problems 90
  solving software upgrade problems 93
  solving web interface problems 91

U

UDP 117
unit, restarting 22
user name
  changing 29
  default 30, 31

V

virtual LAN, testing 61
voice coding algorithm, setting 47
VoIP 118

W

Web browser, choosing suitable 17
web page
  Advanced Debug 19
  Change Password/User Name 18, 29
  Configuration 17, 18
  Overview 18
what’s new in this version v

© Siemens AG 2001.
All rights reserved.
Subject to availability.
Right of modification reserved.

Information and Communication Networks
Hofmannstraße 51, D-81359 München

Siemens Aktiengesellschaft

Order No.: A30817-X3001-A101-1-7619
Printed in the Federal Republic of Germany